CONSEIL D'ÉTAT
section de législation

avis 71.184/4
du 25 avril 2022

sur

des amendements à un projet de loi 'relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités'

RAAD VAN STATE
afdeling Wetgeving

advies 71.184/4
van 25 april 2022

over

amendementen op een wetsontwerp 'betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten'

‡LW-AGFWNFIFE-HBBIEUQ‡

Le 14 mars 2022, le Conseil d'État, section de législation, a été invité par le Vice-Premier Ministre et Ministre de la Justice et de la Mer du Nord à communiquer un avis, dans un délai de trente jours, sur des amendements à un projet de loi 'relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités'.

Les amendements ont été examinés par la quatrième chambre le 25 avril 2022. La chambre était composée de Martine BAGUET, président de chambre, Luc CAMBIER et Bernard BLERO, conseillers d'État, Sébastien VAN DROOGHENBROECK et Jacques ENGLEBERT, assesseurs, et Charles-Henri VAN HOVE, greffier assumé.

Le rapport a été présenté par Anne VAGMAN, premier auditeur chef de section, et Julien GAUL, auditeur adjoint.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Martine BAGUET.

L'avis, dont le texte suit, a été donné le 25 avril 2022.

*

Op 14 maart 2022 is de Raad van State, afdeling Wetgeving, door de Vice-eersteminister en Minister van Justitie en Noordzee verzocht binnen een termijn van dertig dagen een advies te verstrekken over amendementen op een wetsontwerp 'betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten'.

De amendementen zijn door de vierde kamer onderzocht op 25 april 2022. De kamer was samengesteld uit Martine BAGUET, kamervoorzitter, Luc CAMBIER en Bernard BLERO, staatsraden, Sébastien VAN DROOGHENBROECK en Jacques ENGLEBERT, assessoren, en Charles-Henri VAN HOVE, toegevoegd griffier.

Het verslag is uitgebracht door Anne VAGMAN, eerste auditeur-afdelingshoofd, en Julien GAUL, adjunct-auditeur.

De overeenstemming tussen de Franse en de Nederlandse tekst van het advies is nagezien onder toezicht van Martine BAGUET.

Het advies, waarvan de tekst hierna volgt, is gegeven op 25 april 2022.

*

‡LW-AGFWNFIFE-HBBIEUQ‡

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 2°, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973, la section de législation limite son examen au fondement juridique de l'avant-projet ‡, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, les amendements appellent les observations suivantes.

OBSERVATION PRÉALABLE

Eu égard aux nombreux dossiers actuellement soumis à l'avis de la section de législation du Conseil d'État et à la teneur des amendements, ainsi qu'au caractère hautement technique de plusieurs des dispositions examinées, la section de législation n'a pas été en mesure de procéder à un examen exhaustif des amendements, même limité aux trois points indiqués dans l'article 84, § 3, alinéa 1er, des lois 'sur le Conseil d'État', coordonnées le 12 janvier 1973.

Pour tous les aspects qui ne sont pas couverts par le présent avis, la section de législation renvoie à son avis n° 69.381/4 donné le 28 juin 2021 sur l'avant-projet, devenu projet de loi 'relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités' [1] (ci-après : « le projet de loi »), auquel plusieurs amendements à l'examen entendent apporter des modifications.

Enfin, la section de législation rappelle que sa saisine est limitée, par définition, aux textes en projet et qu'il ne lui appartient pas, dans ces conditions, d'examiner si l'ensemble du droit positif belge est de nature à garantir le respect du droit à la vie privée dans la collecte et l'usage qui seraient faits des données dont la conservation est ici prévue. Ainsi, la compatibilité de la chaine de collecte, de conservation, d'accès et d'utilisation des données concernées avec les libertés et droits fondamentaux en cause, dépend d'autres dispositions en vigueur, qu'elles aient ou non une portée générale, dont la section de législation n'est pas saisie dans la présente demande d'avis.

Il va de soi que, dans les conditions qui viennent d'être exposées, il ne peut rien être déduit de ce que, dans le présent avis, aucune observation ne soit formulée sur certaines dispositions ou certaines questions.

‡ S'agissant d'amendements à un projet de loi, on entend par « fondement juridique » la conformité aux normes supérieures.

[1] *Doc. parl.*, Chambre, 2021-2022, n° 55-2572/1, pp. 219 à 320, http://www.raadvst-consetat.be/dbx/avis/69381.pdf. L'avant-projet a été déposé à la Chambre des représentants le 17 mars 2022.

‡LW-AGFWNFIFE-HBBIEUQ‡

PORTÉE DES AMENDEMENTS [2]

I. Contexte jurisprudentiel

A. Les arrêts de la Cour de justice de l'Union européenne

1. Dans un arrêt C-207/16 du 2 octobre 2018 [3], la Cour de Justice de l'Union européenne (ci-après : la Cour de justice) a dit pour droit que l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 'concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)' doit être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave.

2. Par un arrêt C-511/18 rendu le 6 octobre 2020 [4], la Cour de justice a dit pour droit que l'article 15, paragraphe 1, de la directive 2002/58/CE doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

En revanche, l'article 15, paragraphe 1, de la directive 2002/58/CE ne s'oppose pas à des mesures législatives

– permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et cette injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;

[2] Les trois derniers amendements ne sont pas numérotés par le demandeur d'avis. Pour les besoins du présent avis, ils seront numérotés, dans la suite des autres amendements, en tant qu'amendements n[os] 16, 17 et 18.

[3] C.J. (gde ch.), arrêt *Ministerio Fiscal*, 2 octobre 2018, C-207/16, ECLI:EU:C:2018:788.

[4] C.J. (gde ch.), arrêt *La Quadrature du Net e.a.*, 6 octobre 2020, C-511/18, ECLI:EU:C:2020:791.

‡LW-AGFWNFIFE-HBBIEUQ‡

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

– permettant, aux fins de la lutte contre la criminalité grave et à fortiori de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services, dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect de conditions matérielles et procédurales et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

3. Enfin, par un arrêt C-746/18 rendu le 2 mars 2021 [5], la Cour de justice a dit pour droit que

– l'article 15, paragraphe 1, de la directive 2002/58/CE doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès à ces données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période ;

[5] C.J. (gde ch.), arrêt *Prokuratuur*, 2 mars 2021, C-746/18, ECLI:EU:C:2021:152. Voir également C.J. (gde ch.), arrêt *G.D.*, 5 avril 2022, C-140/20, ECLI:EU:C:2022:258.

‡LW-AGFWNFIFE-HBBIEUQ‡

– l'article 15, paragraphe 1, de la directive 2002/58/CE doit être interprété en ce sens qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale.

B. Les arrêts de la Cour constitutionnelle

4. Faisant suite aux arrêts précités de la Cour de justice, la Cour constitutionnelle a rendu, le 22 avril 2021, l'arrêt n° 57/2021 avec la motivation suivante :

« B.15. Il ressort de l'arrêt de la Cour de justice du 6 octobre 2020 en cause, *La Quadrature du Net et autres*, précité, que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, sauf dans les hypothèses limitées décrites par l'arrêt précité.

En ce qu'elle prévoit, par principe et sans limitation à ces hypothèses, une conservation généralisée et indifférenciée, par les opérateurs et fournisseurs de services de communications électroniques, des données d'identification, des données d'accès et de connexion, ainsi que des données de communication, visées à l'article 126, § 3, de la loi du 13 juin 2005 ['relative aux communications électroniques'], la loi attaquée viole par conséquent l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des dispositions précitées de la Charte des droits fondamentaux de l'Union européenne, et en combinaison avec les articles 10 et 11 de la Constitution.

B.16.1. Dans le dispositif de l'arrêt du 6 octobre 2020 en cause *La Quadrature du Net et autres*, précité, la Cour de justice précise cependant que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, ne s'oppose pas à divers types de mesures législatives que la Cour énumère. Sont ainsi admissibles, notamment, des mesures législatives 'prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire', ou encore des mesures législatives 'prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques'. Ces mesures législatives doivent assurer, 'par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus'.

‡LW-AGFWNFIFE-HBBIEUQ‡

B.16.2. Sur la base de ces précisions de la Cour de justice, le Conseil des ministres soutient dans ses mémoires complémentaires qu'en tout état de cause, la loi attaquée ne doit pas être annulée en ce qu'elle prévoit l'obligation généralisée et indifférenciée de conservation, par les opérateurs et fournisseurs de services de communications électroniques, des adresses IP attribuées à la source d'une connexion, d'une part, et des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, d'autre part.

Le Conseil des ministres en conclut que seuls doivent être annulés, le cas échéant, les alinéas 2 et 3 de l'article 126, § 3, de la loi du 13 juin 2005, qui visent respectivement les données de connexion et de localisation et les données de communication. Il estime que l'alinéa 1er de l'article 126, § 3, précité, qui vise les données d'identification, ne doit en revanche pas être annulé, pas plus que les autres dispositions de la loi attaquée, dès lors qu'elles contiennent les garanties nécessaires en termes de conservation des données et d'accès à celles-ci.

B.17. En l'espèce, il y a lieu de constater que la loi attaquée repose, dans son principe même, sur une obligation de conservation généralisée et indifférenciée de l'ensemble des données visées à l'article 126, § 3, de la loi du 13 juin 2005, et qu'elle poursuit, d'une manière générale, comme il est dit en B.3 et en B.4, des objectifs plus larges que la lutte contre la criminalité grave ou le risque d'atteinte à la sécurité publique.

La distinction que l'article 126, § 3, de la loi du 13 juin 2005 opère entre trois catégories de données (à savoir : les données d'identification, les données d'accès et de connexion, ainsi que les données de communication) n'a d'incidence que sur le point de départ de la durée de conservation des données, de douze mois en toute hypothèse, et éventuellement sur les possibilités d'accéder à celles-ci, pour les instances habilitées (voy. l'article 46*bis* du Code d'instruction criminelle et l'article 126, § 2, de la loi du 13 juin 2005). Cette catégorisation ne correspond par ailleurs pas aux distinctions qui sont opérées par la Cour de justice dans son arrêt du 6 octobre 2020 en ce qui concerne les différentes catégories de données susceptibles de faire l'objet d'une obligation de conservation généralisée et indifférenciée, moyennant le respect de plusieurs conditions (à savoir, en l'occurrence : les adresses IP attribuées à la source d'une connexion et les données relatives à l'identité civile des utilisateurs de moyens de communications électroniques).

B.18. L'arrêt de la Cour de justice du 6 octobre 2020 impose un changement de perspective par rapport au choix que le législateur a effectué : l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle. La réglementation prévoyant une telle obligation doit par ailleurs être soumise à des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales (point 133). Cette réglementation doit garantir que l'ingérence se limite au strict nécessaire et doit toujours 'répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi' (points 132 et 133).

‡LW-AGFWNFIFE-HBBIEUQ‡

B.19. Il appartient au législateur d'élaborer une réglementation qui respecte les principes applicables en matière de protection des données à caractère personnel, à la lumière de la jurisprudence de la Cour de justice, et de tenir compte, le cas échéant, des précisions apportées par celle-ci en ce qui concerne les différents types de mesures législatives jugées compatibles avec l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8, 11 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne. En particulier, il appartient également au législateur, dans ce contexte, d'opérer les distinctions qui s'imposent entre les différents types de données soumises à conservation, de manière à garantir que, pour chaque type de donnée, l'ingérence soit limitée au strict nécessaire.

B.20. Compte tenu de ce qui précède, il y a lieu d'annuler les articles 2, b), 3 à 11 et 14 de la loi attaquée, qui sont indissociablement liés ».

5. Dans ce contexte, les auteurs du projet de loi auquel les amendements se rapportent ont dès lors décidé d'adopter un dispositif qui a pour objet de mettre en place un système de conservation des données qui permettraient d'atteindre les objectifs dont la Cour de justice et la Cour constitutionnelle ont reconnu le caractère légitime, tout en se conformant aux décisions de ces hautes juridictions, dans leur dispositif et leur motivation, en particulier les limites et critères qui résultent de celles-ci en matière de conservation des données de trafic et de localisation par les opérateurs intervenant dans le secteur des communications électroniques, et d'accès à ces données par les autorités.

6. Par un arrêt n° 158/2021 du 18 novembre 2021, la Cour constitutionnelle a annulé l'article 2 de la loi du 1er septembre 2016 'portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité' , uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération.

La disposition annulée énonce :

« Dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, modifié par les lois des 4 février 2010, 10 juillet 2012, 27 mars 2014 et 29 mai 2016, les modifications suivantes sont apportées :

1° dans le paragraphe 1er, les modifications suivantes sont apportées :

[…]

c) sept alinéas rédigés comme suit sont insérés entre les alinéas 1er et 2 :

'Pour ce qui concerne l'identification de l'utilisateur final, l'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er, est le responsable du traitement au sens de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques.

Lorsque l'utilisateur final présente un document d'identification comprenant le numéro de registre national, l'opérateur, le fournisseur visé à l'article 126, § 1er, alinéa 1er, le canal de vente de services de communications électroniques ou l'entreprise fournissant un service d'identification collecte ce numéro.

‡LW-AGFWNFIFE-HBBIEUQ‡

Le canal de vente de services de communications électroniques ne conserve pas de données ou de documents d'identification, qui sont transmis à l'opérateur, au fournisseur visé à l'article 126, § 1er, alinéa 1er ou à l'entreprise fournissant un service d'identification.

Si une introduction directe dans les systèmes informatiques de l'opérateur, du fournisseur visé à l'article 126, § 1er, alinéa 1er ou de l'entreprise fournissant un service d'identification n'est pas possible, le canal de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques.

L'opérateur ou le fournisseur visé à l'article 126, § 1er, alinéa 1er conserve une copie des documents d'identification autres que la carte d'identité électronique belge.

Les données et documents d'identification collectés sont conservés conformément à l'article 126, § 3, alinéa 1er'.

[…] ».

La décision de la Cour constitutionnelle est motivée comme suit :

« Quant au premier moyen

[…]

B.8.4.1. Pour ce qui est des données d'identification et des documents d'identification concernés, l'article 127 de la loi attaquée dispose qu'il doit s'agir de documents comportant le numéro de registre national et que le numéro de registre national est une donnée à caractère personnel qui doit être collectée et traitée dans ce contexte. Les autres données d'identification, ainsi que les documents d'identification qui entrent en considération, ne sont pas énumérés dans cette disposition législative, en dépit des avis mentionnés en B.8.1.

B.8.4.2. En outre, le législateur n'a pas donné au Roi une habilitation explicite pour définir plus précisément ces données d'identification et ces documents d'identification. De tels éléments essentiels d'un traitement de données à caractère personnel ne sauraient toutefois être couverts par l'habilitation vague conférée par l'article 127, § 1er, alinéa 1er, de la loi du 13 juin 2005 et qui consiste à prendre les 'mesures techniques et administratives' nécessaires en vue de l'identifiabilité de l'utilisateur final.

Le Roi devait dès lors déterminer ces données et ces documents d'identification sur la base du pouvoir qu'Il tire de l'article 108 de la Constitution de faire les règlements et les arrêtés nécessaires pour l'exécution des lois.

Toutefois, ce pouvoir général d'exécution du Roi ne saurait suffire en l'espèce. En effet, la délégation d'éléments essentiels d'une matière réservée par le Constituant au pouvoir législatif n'est possible que si le respect de la procédure parlementaire ne permet pas au législateur de réaliser un objectif d'intérêt général et à condition qu'il détermine explicitement et sans équivoque l'objet de cette habilitation et que les mesures prises par le Roi soient examinées par le pouvoir législatif, en vue de leur confirmation, dans un délai relativement court, fixé dans la loi d'habilitation.

B.8.4.3. Lors des travaux préparatoires, le législateur justifie cette méthode de travail par le caractère technique des données d'identification et des documents d'identification, la nécessité de pouvoir en adapter l'énumération en fonction de nouveaux enseignements et le fait que, dans le cadre de la conservation des données, ces données n'étaient pas non plus énumérées dans l'article 126 de la loi du 13 juin 2005 lui-même annulé par l'arrêt de la Cour n° 57/2021 du 22 avril 2021.

‡LW-AGFWNFIFE-HBBIEUQ‡

Indépendamment du fait que ces arguments ne sauraient expliquer l'absence d'une habilitation explicite et sans équivoque, le caractère technique des données d'identification et des documents d'identification et l'adaptabilité d'une telle énumération ne suffisent pas pour conclure que le fait d'ancrer de tels éléments dans une norme législative ne permettrait pas au législateur de réaliser un objectif d'intérêt général. En effet, même une norme législative peut être modifiée. Le Conseil des ministres ne démontre pas qu'une modification de ces données d'identification peut être urgente au point de ne pas pouvoir suivre le cours normal de la procédure législative. De même, une énumération des données d'identification et des documents d'identification n'est pas complexe au point de ne pas pouvoir être inscrite dans une norme législative. Enfin, le législateur ne saurait justifier une violation de la Constitution en renvoyant à une autre disposition législative qui comportait peut-être la même inconstitutionnalité.

B.8.4.4. Au demeurant, l'article 127 de la loi du 13 juin 2005 délimite insuffisamment le pouvoir d'exécution du Roi pour déterminer les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération. En ce qui concerne les documents d'identification, il mentionne seulement qu'il doit s'agir de documents comprenant le numéro de registre national. En ce qui concerne les données d'identification autres que le numéro de registre national, il ne comporte pas la moindre précision.

[…]

B.9.1. Il ressort de ce qui précède que l'article 127 de la loi du 13 juin 2005, tel qu'il a été modifié par l'article 2 de la loi attaquée, viole le principe de légalité garanti par l'article 22 de la Constitution, mais seulement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération. Dans cette mesure, il y a lieu d'annuler l'article 2 de la loi attaquée.

[…]

B.9.3. Étant donné que la violation constatée porte uniquement sur l'article 22 de la Constitution et non sur les normes du droit de l'Union européenne invoquées dans le moyen, il appartient à la Cour, en vertu de l'article 8, alinéa 3, de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, d'indiquer ceux des effets des dispositions annulées qui doivent être considérés comme définitifs ou maintenus provisoirement pour le délai qu'elle détermine.

La violation constatée de l'article 22 de la Constitution ne porte pas sur la nature et le contenu des données d'identification ou des documents d'identification tels qu'ils sont actuellement réglés dans l'arrêté royal du 27 novembre 2016 et tels qu'ils échappent au pouvoir de contrôle de la Cour. Elle porte uniquement sur le fait que ces données et documents doivent être énumérés dans une disposition législative.

Il y a donc lieu de donner au législateur le temps nécessaire pour prévoir ce fondement légal, sans qu'il faille dans l'intervalle annuler l'identification des utilisateurs finaux de cartes de téléphonie mobile prépayées réglée par la disposition attaquée. En outre, ce délai doit être suffisamment long pour permettre au législateur d'aligner ce fondement légal sur la nouvelle réglementation en matière de conservation des données qui est en préparation, à la suite de l'arrêt de la Cour n° 57/2021 du 22 avril 2021.

Par conséquent, il y a lieu de maintenir les effets de la disposition attaquée comme il est indiqué dans le dispositif.

Quant au deuxième moyen

[…]

‡LW-AGFWNFIFE-HBBIEUQ‡

B.15.2. La loi présentement attaquée, en revanche, porte uniquement sur les données visées à l'article 127 de la loi du 13 juin 2005, à l'aide desquelles l'utilisateur final d'un service de communications électroniques fourni sur la base d'une carte de téléphonie mobile prépayée peut être identifié. L'article 12, alinéa 2, de l'arrêté royal du 27 novembre 2016 dispose que ces données d'identification peuvent varier en fonction de la méthode d'identification choisie, mais il énumère par la même occasion limitativement les données d'identification que l'entreprise concernée peut conserver au maximum :

'1° le nom et le prénom ;

2° le sexe ;

3° la nationalité ;

4° la date et le lieu de naissance ;

5° l'adresse du domicile, l'adresse e-mail et le numéro de téléphone ;

6° le numéro de registre national ;

7° le numéro du document d'identité, le pays d'émission du document lorsqu'il s'agit d'un document étranger et la date de validité du document ;

8° les références de l'opération de paiement conformément à l'article 17 ;

9° l'association de la carte prépayée au produit pour lequel l'utilisateur final est déjà identifié conformément à l'article 18 ;

10° la photo de l'utilisateur final, mais uniquement pour les documents autres que la carte d'identité électronique belge'.

Compte tenu de l'annulation partielle visée en B.9.1 et du maintien des effets visé en B.9.3, le législateur doit, avant la date mentionnée dans le dispositif, inclure dans une disposition législative les données d'identification et les documents d'identification qui peuvent servir à l'application de l'article 127 de la loi du 13 juin 2005.

B.15.3. Ces données personnelles ne sont pas des données relatives au trafic et des données de localisation, mais uniquement les données qui sont habituellement utilisées pour identifier une personne. Il n'est pas possible, à l'aide de ces seules données, de suivre les déplacements, les communications, les activités ou les relations sociales de cette personne, ni d'établir un profil personnel permettant de tirer des conclusions précises sur son orientation sexuelle, ses convictions et son état de santé. En soi, elles ne divulguent donc pas d'informations sensibles sur la vie privée.

Il est exact que ces données d'identification peuvent ensuite être associées à d'autres données et contribuer, de cette manière, à la divulgation de telles informations sensibles sur la vie privée d'une personne. Ces autres données doivent toutefois, dans ce cas, être collectées d'une autre manière et cette collecte doit elle aussi s'effectuer dans le respect de la législation applicable et des droits fondamentaux de l'intéressé.

Par conséquent, il y a lieu d'apprécier la compatibilité de la loi attaquée avec le droit au respect de la vie privée à l'aide des critères mentionnés en B.14.3.

B.16.1. Les conditions matérielles et procédurales de la collecte, du traitement et de la conservation des données d'identification des utilisateurs finaux d'un réseau de communications électroniques sur la base d'une carte de téléphonie mobile prépayée sont réglées dans les articles 126 et 127 de la loi du 13 juin 2005 et dans les arrêtés royaux du 19 septembre 2013 et du 27 novembre 2016.

[…]

‡LW-AGFWNFIFE-HBBIEUQ‡

B.16.8.5. Ces dispositions règlent de manière claire et précise les conditions matérielles et procédurales auxquelles ces autorités peuvent avoir accès aux données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005.

Lorsqu'elles accèdent à ces données, ces autorités doivent respecter non seulement les règles mentionnées en B.16.8.2 à B.16.8.4, mais aussi les droits fondamentaux de l'utilisateur final, garantis notamment par le [règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après « RGPD »)], par les articles 6 et 8 de la Convention européenne des droits de l'homme et par les articles 7, 8 et 47 de la Charte.

B.16.8.6. À cet égard, les parties requérantes renvoient à l'arrêt de la grande chambre de la Cour de justice du 2 mars 2021 en cause *Prokuratuur* (C-746/18, points 50 à 56), dans lequel la Cour de justice exige, selon elles, qu'une autorité administrative indépendante ou un juge contrôle au préalable chaque demande d'accès au regard des droits fondamentaux et règles nationales applicables et dans lequel elle précise, selon les parties requérantes, que le ministère public, qui dirige la procédure d'enquête et exerce le cas échéant l'action publique, ne dispose pas de l'indépendance requise pour pouvoir effectuer ce contrôle.

Toutefois, cet arrêt portait sur une demande du ministère public d'obtenir un accès à des données relatives au trafic et à des données de localisation. Comme il est dit en B.14.3, la Cour de justice et la Cour européenne des droits de l'homme n'exigent en revanche pas de contrôle judiciaire ou administratif préalable pour une demande d'accès à des données d'identification. En conséquence, le droit au respect de la vie privée ne s'oppose pas à une demande d'accès à de telles données qui émane du ministère public.

B.16.8.7. Cela étant, la demande d'accès aux données d'identification traitées en vertu de l'article 127 de la loi du 13 juin 2005 doit toujours être motivée *in concreto* par la démonstration du lien entre ces données et les éléments objectifs qui fondent la suspicion concrète initiale à l'égard de l'utilisateur final en question concernant une infraction spécifique. Il faut également motiver le fait que l'on ne demande pas davantage de données que celles qui sont strictement nécessaires dans le cadre de l'enquête en cours. Une telle motivation ne peut pas recourir à des formulations types ou à des formules de style.

[…]

B.22. L'article 127 de la loi du 13 juin 2005 porte uniquement sur la conservation et le traitement des données d'identification visées à l'article 12 de l'arrêté royal du 27 novembre 2016. À elles seules, ces données ne donnent pas d'information sur les opinions personnelles de la personne identifiée. De même, les données relatives au trafic et les données de localisation auxquelles elles pourraient être associées ne constituent pas en soi l'expression d'une opinion.

Ce n'est que si ces données étaient également liées au contenu d'une communication effectuée et que l'analyse de celles-ci entrainait d'autres mesures, telles qu'une enquête par les services de renseignement et de sécurité ou une instruction pénale, qu'il pourrait en résulter une limitation de la liberté d'expression, de la liberté d'obtenir des informations, de la liberté de presse ou du secret des sources.

Comme il est dit en B.15.3, une association des données d'identification à d'autres métadonnées ou au contenu d'une communication doit toutefois être fondée sur une disposition législative claire et sans équivoque, respecter les conditions matérielles et procédurales de cette disposition et être compatible avec les droits fondamentaux de l'intéressé.

‡LW-AGFWNFIFE-HBBIEUQ‡

Un tel lien indirect entre la suppression, attaquée, de l'anonymat des cartes de téléphonie mobile prépayées et le contenu des communications effectuées ne suffit pas pour considérer que la loi attaquée limite la liberté d'expression. La simple collecte de données d'identification de tous les utilisateurs finaux d'un réseau de communications électroniques ne saurait justifier la crainte, dans un État de droit démocratique, que toutes les communications menées sur ce réseau seront supervisées par les pouvoirs publics. La loi attaquée ne saurait dès lors avoir pour effet, par elle-même, de dissuader des personnes d'exprimer leur opinion ou de partager des informations avec des journalistes ou avec des personnalités politiques.

[…]

Quant au troisième moyen

[…]

B.24.3. La disposition attaquée n'incrimine aucun comportement et ne définit pas de peines pour des infractions spécifiques. Contrairement à ce que les parties requérantes font valoir, elle n'impute pas non plus automatiquement à l'utilisateur final d'une carte de téléphonie mobile prépayée qui a été identifié les infractions qui sont découvertes ou prouvées à la suite de l'analyse de l'utilisation de cette carte de téléphonie mobile. L'article 127, § 1er, alinéa 3, de la loi du 13 juin 2005 contient seulement la présomption réfragable selon laquelle cet utilisateur final est également celui qui utilise cette carte de téléphonie mobile. Le principe de légalité en matière pénale n'est pas applicable à une telle disposition.

B.26.2. La disposition attaquée n'établit dès lors pas de responsabilité pénale automatique ou de responsabilité objective de l'utilisateur final d'une carte de téléphonie mobile prépayée qui a été identifié en ce qui concerne l'utilisation qu'en fait un tiers. Elle remplit principalement une fonction d'avertissement, étant donné qu'elle rappelle la présomption de départ de toute enquête pénale et de toute enquête par les services de renseignement et de sécurité, à savoir la présomption selon laquelle c'est le propriétaire ou l'utilisateur habituel d'un objet qui l'a utilisé pour commettre l'infraction ou pour menacer la sécurité nationale. Les enquêteurs écartent cette présomption dès qu'elle est infirmée par les éléments de preuve recueillis.

B.26.3. La disposition attaquée est donc en rapport avec les objectifs que poursuit le législateur par l'article 127 de la loi du 13 juin 2005, à savoir ceux qui portent sur des situations et des enquêtes urgentes.

B.26.4. En outre, la disposition attaquée est souvent appliquée dans le cadre d'infractions ou de menaces pour la sécurité nationale susceptibles d'avoir des conséquences graves sur l'intégrité physique de personnes ou de causer des troubles sociétaux considérables.

B.26.5. L'utilisateur final identifié dispose de plusieurs possibilités pour se défendre dans le cadre des poursuites pénales qui pourraient découler de l'utilisation de sa carte de téléphonie mobile prépayée faite par un tiers. S'il informe les enquêteurs de la personne qui a utilisé sa carte de téléphonie mobile prépayée, ceux-ci doivent examiner l'implication de cette personne.

Du reste, la disposition attaquée se contente d'instaurer une présomption réfragable, que le prévenu peut contester par toutes voies de droit. Elle ne lui interdit pas de présenter tous les éléments de fait qui infirment son implication dans les infractions commises ou dans les menaces pour la sécurité nationale qui font l'objet d'une enquête.

‡LW-AGFWNFIFE-HBBIEUQ‡

Par ailleurs, la disposition attaquée n'enlève rien au principe selon lequel il revient au ministère public, dans un procès pénal, de prouver la culpabilité du prévenu. Il appartient au juge répressif d'apprécier la valeur probante de tous les éléments de preuve, en ce compris les explications du prévenu, en respectant son droit à un procès équitable.

La disposition attaquée ne portant donc pas atteinte aux droits de défense du prévenu, elle ne compromet pas non plus la présomption d'innocence.

B.26.6. Contrairement à ce que les parties requérantes font valoir, ce qui précède vaut tout autant pour l'implication de l'utilisateur final identifié dans les infractions terroristes mentionnées aux articles 137 à 141*ter* du Code pénal. Il ne peut être condamné en tant que coauteur ou complice de telles infractions que si le ministère public démontre à son encontre que tous les éléments constitutifs de ces infractions, y compris l'élément intentionnel, sont réunis en ce qui le concerne. La mise à disposition de bonne foi d'une carte de téléphonie mobile prépayée par un utilisateur final qui ne pouvait pas présumer qu'elle serait utilisée pour commettre ou pour préparer une telle infraction ne saurait justifier en soi une condamnation pénale.

[…]

Quant au quatrième moyen

[…]

B.29.1. L'accès d'une autorité aux données bancaires relève du champ d'application du droit au respect de la vie privée, indépendamment du fait que ces données soient sensibles ou non ou qu'elles aient un rapport ou non avec l'exercice de la profession (CEDH, 7 juillet 2005, *M.N. e.a. c. Saint-Marin*, §§ 51-55 ; 1er décembre 2015, *Brito Ferrinho Bexiga Villa-Nova c. Portugal*, § 44 ; 27 avril 2017, *Sommer c. Allemagne*, § 48).

B.29.2. L'accès de l'autorité publique aux données bancaires doit être basé sur une habilitation légale spécifique qui en délimite clairement et sans équivoque l'objet ainsi que le seuil pour y accéder. Cet objet doit être limité à ce qui est nécessaire au regard de l'objectif légitime poursuivi, étant donné qu'un accès trop large aux données bancaires permettrait à l'autorité publique de se faire une idée détaillée de la vie privée de l'intéressé. L'autorité publique ne peut avoir accès à de telles données que si elle dispose d'indices concrets que le titulaire du compte bancaire est impliqué dans une infraction. La loi doit également prévoir des mesures contre les abus, parmi lesquelles la garantie que les données ne seront pas conservées plus longtemps que ce qui est nécessaire aux fins de l'investigation menée. Enfin, il doit exister un contrôle juridictionnel effectif du respect de ces garanties matérielles et procédurales (CEDH, 27 avril 2017, *Sommer c. Allemagne*, §§ 57-63).

B.30.1. La disposition attaquée précise les services qui disposent de l'habilitation visée en B.28.2 et les institutions qui sont tenues d'apporter leur concours.

Elle délimite également de deux manières l'objectif de la mesure attaquée. Premièrement, elle vise à identifier soit l'utilisateur final d'une carte de téléphonie mobile prépayée visé à l'article 127 de la loi du 13 juin 2005, soit la carte de téléphonie mobile prépayée qui est utilisée par une certaine personne. Deuxièmement, cette identification doit s'inscrire dans le cadre des missions des services de renseignement et de sécurité.

B.30.2. L'objet de l'acte d'investigation est limité à une transaction bancaire spécifique, à savoir celle qui a permis d'acheter une carte de téléphonie mobile prépayée. Un tel acte d'investigation ne permet aux services de renseignement et de sécurité que de recueillir des données d'identification, mais ne leur fournit pas à lui seul des données relatives au trafic ou des données de localisation, ni un accès aux communications effectuées.

‡LW-AGFWNFIFE-HBBIEUQ‡

La disposition attaquée ne leur permet pas non plus d'obtenir, par ce seul acte d'investigation, d'autres informations financières relatives au titulaire du compte bancaire. Elle ne leur permet donc pas, à l'aide des seules données d'identification obtenues, de se faire une idée de ses habitudes de dépenses faites par le titulaire du compte bancaire ou de toute autre information personnelle sensible le concernant.

Comme il est dit en B.15.3, s'il est vrai que ces données d'identification peuvent ensuite être associées à d'autres données et que la disposition attaquée peut ainsi contribuer à la divulgation de telles informations sensibles, ces informations doivent alors être recueillies à l'aide d'autres actes d'investigation, qui doivent à leur tour respecter la législation applicable et les droits fondamentaux de l'intéressé.

B.30.3. Comme il est dit en B.3.3, l'identification sur la base de la disposition attaquée peut s'avérer nécessaire en fonction de la méthode d'identification que l'utilisateur final a choisie lors de l'achat de la carte de téléphonie mobile prépayée.

Si, lors de l'achat de la carte de téléphonie mobile prépayée, il opte pour l'identification sur la base de l'opération de paiement en ligne, les services de renseignement et de sécurité ne peuvent l'identifier que s'ils disposent de la référence de la transaction bancaire électronique et qu'ils peuvent l'associer tant à la carte de téléphonie mobile qu'à l'identité de l'utilisateur final (*Doc. parl.*, Chambre, 2015-2016, DOC 54-1964/001, pp. 14-16).

[…]

B.30.4. Étant donné que la disposition attaquée n'habilite les services de renseignement et de sécurité qu'à effectuer l'acte d'investigation attaqué 'dans l'intérêt de l'exercice de leurs missions', ceux-ci doivent toujours disposer, à cet effet, d'indices concrets que l'identification de l'utilisateur final d'une carte de téléphonie mobile prépayée est nécessaire dans le cadre des missions énumérées limitativement à l'article 7 (Sureté de l'État) et à l'article 11 (Service général du renseignement et de la sécurité) de la loi du 30 novembre 1998. Ces missions portant toutes sur des intérêts vitaux de la Nation, le fait de prendre une telle mesure suppose toujours au moins un risque que se produise un événement qui aurait des conséquences sociétales très graves.

[…]

Par ces motifs,

la Cour,

– annule l'article 2 de la loi du 1er septembre 2016 'portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité', uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération ;

– maintient les effets de la disposition annulée jusqu'à l'entrée en vigueur d'une norme législative qui énumère ces données d'identification et ces documents d'identification et au plus tard jusqu'au 31 décembre 2022 inclus ;

– rejette le recours pour le surplus, sous réserve des interprétations mentionnées en B.8.7.3, B.16.6, B.16.8.5, B.16.8.7, B.26.2, B.26.6 et B.30.4 ».

‡LW-AGFWNFIFE-HBBIEUQ‡

II. Portée des amendements

L'auteur des amendements résume leur portée comme suit :

« 1. Introduction et/ou rétroactes

Notre Cour constitutionnelle a, dans son arrêt n° 57/2021 du 22 avril 2021, annulé les articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 'relative à la collecte et à la conservation des données dans le secteur des communications électroniques'. Cette loi est connue sous le nom de 'data retention'.

Cette loi prévoyait l'obligation pour les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'internet et de courrier électronique par internet (qu'ils soient opérateurs notifiés à l'IBPT ou non) de conserver certaines données d'identification, de localisation et de trafic pendant une durée de 12 mois, afin que ces données soient disponibles pour des finalités répressives (enquêtes pénales) ou pour l'accomplissement des missions des services de renseignement et de sécurité. Ces données ne concernent pas le contenu des communications.

Le gouvernement a finalisé un projet de réparation de la loi 'data retention'. Ce projet a été approuvé par le Conseil des ministres du 17/12/2021 (deuxième lecture). Ce projet a reçu tous les avis nécessaires et le gouvernement avait donc l'intention de le déposer dès que possible au Parlement.

Cependant, notre Cour constitutionnelle a entre-temps rendu le 18/11/2021 un nouvel arrêt concernant la loi du 1er septembre 2016, qui avait été adoptée pour mettre fin à l'anonymat des abonnés de cartes prépayées qui permettent d'utiliser des services mobiles (téléphoner, accéder à internet, envoyer des SMS, etc.), en obligeant les opérateurs à identifier ces derniers. Dans cet arrêt, la Cour :

– ne remet pas en cause le principe d'identification des abonnés de cartes prépayées ;

– mais annule le changement fait par la loi du 1er septembre 2016 à l'art. 127 de la loi télécom 'uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération' ; selon la Cour, l'article 22 de la Constitution exige que ces données et documents soient énumérés dans la loi ;

– maintient les effets de la disposition annulée jusqu'à l'entrée en vigueur d'une norme législative qui énumère ces données d'identification et ces documents d'identification et au plus tard jusqu'au 31 décembre 2022 inclus.

Il ressort de l'analyse effectuée que les articles 126 et 126/1 de la loi télécom, tels qu'envisagés dans le projet de réparation, doivent effectivement être revus. En effet, il serait paradoxal et difficilement justifiable :

– que les données d'identification que les opérateurs doivent conserver sur base de l'article 126 de la loi télécom soient fixés par arrêté royal, alors que les données d'identification qu'ils doivent conserver sur base de l'article 127 de la loi doivent, selon la Cour constitutionnelle, être listées dans la loi ;

– de reprendre dans la loi les données d'identification visées par l'article 127 mais que des métadonnées (ex. qui appelle qui à quel moment et les données de localisation), qui devront être conservées sur base de l'article 126/1 de la loi télécom et qui doivent être considérées comme plus intrusives à l'égard de la vie privée des personnes concernées (dès lors qu'elles dévoilent plus d'informations sur leurs habitudes de vie) que de simples données d'identification, puissent être listées dans un arrêté royal.

Il en résulte que le projet de réparation doit être modifié en ces articles 126 à 127.

‡LW-AGFWNFIFE-HBBIEUQ‡

2. Exposé du dossier

2.1. Amendements à la loi télécom pour ce qui concerne les articles 126 et 126/1

Il est renvoyé au point 1 ci-dessus. Les données à conserver par les opérateurs, actuellement listées dans l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi télécom, ont été transférées vers les articles 126 et 126/2 de la loi télécom. Les données à conserver en vertu de l'article 126/1 ont été reprises dans un nouvel article 126/2, l'article 126/1 étant déjà particulièrement long.

Il convient dès lors d'adapter les modifications projetées à l'arrêté royal du 19 septembre 2013, qui est vidée d'une grande partie de sa substance.

2.2. Amendements à l'article 127 de la loi télécom et des articles liés

Il est répondu à l'arrêt de la Cour constitutionnelle du 18/11/2021 en modifiant l'article 127 de la loi télécom, de sorte que cet article énumère désormais les données et documents d'identification prévus.

2.3. Amendements de certaines lois organiques

L'actuel article 127 de la loi télécom a été exécuté par l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée (ci-après l'arrêté royal 'cartes prépayées'). Cet arrêté royal prévoit plusieurs méthodes d'identification directe de l'abonné (l'opérateur collecte directement auprès de l'utilisateur/abonné l'identité civile de celui-ci) et une méthode d'identification indirecte de l'abonné. Par exemple, en cas de paiement en ligne d'une carte prépayée, l'opérateur conserve la référence de paiement, que l'autorité fournira à une banque en lui demandant de lui fournir l'identité de l'abonné.

La nouvelle version de l'article 127 établit dorénavant la liste des méthodes d'identification indirecte admises, vu qu'il s'agit d'un point essentiel de la législation.

Certaines de ces méthodes indirectes d'identification nécessitent l'intervention de tiers qui ne sont pas des opérateurs afin de rendre l'identification possible. Il s'agit, en particulier :

– du secteur bancaire (référence de paiement détenue par un opérateur et communiquée à une banque pour obtenir l'identité de l'abonné) ;

– des centres fermés (qui prennent des cartes prépayées pour les personnes de ces centres et font donc à leur niveau le lien entre une carte prépayée et une identité) ;

– des personnes morales qui peuvent jouer un rôle d'intermédiaire dans la distribution des cartes prépayées ou la souscription d'abonnements, notamment pour aider des personnes en situation de vulnérabilité (ex. résidences pour personnes âgées).

Il convient, le cas échéant, de modifier les lois organiques pour s'assurer que les autorités puissent obtenir de ces tiers l'identité de l'abonné sur la base des informations déjà à leur disposition via la méthode indirecte.

Auparavant, tant les services de renseignement et de sécurité que le procureur du Roi pouvaient s'adresser aux banques pour obtenir de l'opérateur l'identité de l'abonné lorsque l'opérateur avait permis d'identifier ses abonnés à l'aide d'une référence de paiement bancaire. Ceci a été confirmé dans le Code d'instruction criminelle et a été étendu aux officiers de police judiciaire de l'IBPT, à la FSMA et à la direction protection de la santé des consommateurs ».

‡LW-AGFWNFIFE-HBBIEUQ‡

FORMALITÉS PRÉALABLES

La demande d'avis renseigne ce qui suit :

« Une consultation publique de 4 semaines, conformément à l'article 18 du Code européen des communications électroniques, a en outre démarré le 25 février 2022 via le site Internet de l'IBPT et l'avis des trois autorités compétentes en matière de protection des données a également été demandé.

À cet égard, nous pouvons d'ores-et-déjà vous communiquer que, vu que ces modifications sous forme d'amendements concernent essentiellement les traitements effectués par les opérateurs (collecte de données d'identification/de localisation), le C.O.C. et le Comité R considèrent qu'ils ne sont pas compétents pour rendre un avis.

L'APD nous a indiqué qu'elle rendrait son avis dans un délai d'un mois (la demande d'avis datant du 25 février 2022).

Enfin, le Comité interministériel des télécommunications, de la radiodiffusion et de la télévision sera consulté et l'accord du Comité de concertation sera également demandé » [6].

Il résulte de ce qui précède que suite à l'accomplissement des formalités obligatoires précitées, le texte soumis pour avis est encore susceptible de subir des modifications autres que celles qui pourraient découler de l'avis de la section de législation.

Or, et même si la section de législation est tenue de se prononcer sur un avant-projet législatif, et ce alors que toutes les formalités préalables obligatoires n'ont pas été accomplies, il s'impose de ne lui soumettre que des projets ou avant-projets de texte à priori définitifs, non seulement pour éviter qu'elle n'examine inutilement un texte qui fera l'objet de modifications ultérieures, mais également pour qu'un projet ne doive lui être soumis à nouveau pour avis en raison de modifications autres que celles résultant de son avis.

L'auteur des amendements est invité à se conformer dorénavant à cette règle [7].

[6] L'avis n° 66/2022 du 1er avril 2022 de l'Autorité de protection des données a été communiqué à la section de législation le 12 avril 2022.

[7] Voir, en ce sens, l'avis n° 69.381/4, p.4.

‡LW-AGFWNFIFE-HBBIEUQ‡

EXAMEN DES AMENDEMENTS

Amendement n° 1
Article 126 en projet de la loi du 13 juin 2005

1. Afin de répondre à la critique de la Cour constitutionnelle dans son arrêt n° 158/2021 du 18 novembre 2021 relative à la violation du principe de légalité consacré à l'article 22 de la Constitution, l'amendement n° 1 entend désormais déterminer, à l'article 126, § 1er, en projet de la loi du 13 juin 2005, les données que doivent conserver les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques qui permettent la fourniture de ces services pour autant qu'ils les traitent ou les génèrent dans le cadre de la fourniture de ces réseaux ou services [8].

Certaines de ces données peuvent être qualifiées de données relatives à l'identité civile des utilisateurs au sens de la jurisprudence de la Cour de justice ou, à tout le moins, de données qui présentent des risques similaires au regard de la vie privée des utilisateurs [9]. Les autres données constituent des données relatives au trafic ou des données de localisation, comme, par exemple, les adresses IP attribuées à la source d'une connexion.

L'accès à ces données, réglé à l'article 127/1, § 3, en projet de la loi du 13 juin 2005, n'apparait à priori pas poser de difficultés au regard du cadre fixé par la Cour de justice.

[8] La plupart de ces données sont actuellement énoncées dans les paragraphes 1er des articles 3 à 6 de l'arrêté royal du 19 septembre 2013 'portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques'.

[9] La Cour de justice a jugé, dans son arrêt C-511/18 : « 157. En ce qui concerne, enfin, les données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, ces données ne permettent pas, à elles seules, de connaitre la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, points 59 et 60).
158. Il en découle que, conformément à ce qui a été exposé au point 140 du présent arrêt, les mesures législatives visant le traitement de ces données en tant que telles, notamment leur conservation et l'accès à celles-ci à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58 (voir, en ce sens, arrêt du 2 octobre 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, point 62) ».

‡LW-AGFWNFIFE-HBBIEUQ‡

L'auteur de l'amendement veillera toutefois à s'assurer que les données reprises à l'article 126, § 1er, en projet, autres que celles relatives à l'identité civile, ne présentent pas de risques similaires, en termes de traçage de l'utilisateur, à ceux évoqués par la Cour de justice en ce qui concerne les adresses IP attribuées à la source de la connexion [10], auquel cas l'accès à ces données devrait également être restreint, à l'instar de ce que prévoit l'article 127/1, § 3, alinéa 4, en projet [11].

Le dispositif sera revu en conséquence.

2. L'article 126, § 1er, alinéa 1er, 17°, et alinéa 2 en projet énonce :

> « Sans préjudice du RGPD et de la loi du 30 juillet 2018, les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques qui permettent la fourniture de ces services, conservent les données suivantes, pour autant qu'ils les traitent ou les génèrent dans le cadre de la fourniture de ces réseaux ou services :
>
> […]
>
> 17° les autres identifiants relatifs à l'utilisateur final, à l'équipement terminal ou à l'équipement le plus proche de cet équipement terminal, qui résultent de l'évolution technologique et qui sont déterminés par le Roi, pour autant que cet arrêté soit confirmé par la loi dans les douze mois suivant la publication de cet arrêté.
>
> L'arrêté royal visé à l'alinéa 1er, 17°, ne porte pas sur le contenu des communications électroniques, ni sur des métadonnées de communications électroniques qui donnent des informations sur le destinataire de la communication, comme l'adresse IP du destinataire de la communication, ou sur la localisation de l'équipement terminal ».

Pour se conformer à l'arrêt n° 158/2021 du 18 novembre 2021 de la Cour constitutionnelle [12], l'auteur de l'amendement démontrera, dans la justification de l'amendement, en quoi le « cours normal de la procédure législative » est tel qu'il ne permet pas de déterminer ces identifiants en temps utile. À cette occasion, il précisera en quoi un délai de douze mois est conforme aux enseignements de l'arrêt précité, qui requiert que la confirmation de l'arrêté ait lieu dans un « délai relativement court ».

---

[10] Voir l'arrêt C-511/18 (considérant 153) et l'arrêt C-746/18 (considérant 35) de la Cour de justice ainsi que, particulièrement en ce qui concerne les données permettant d'identifier techniquement les équipements terminaux des utilisateurs finaux, l'avis n° 108/2021 (considérant 102) et l'avis n° 66/2022 (note de bas de page n° 12), de l'Autorité de protection des données. Voir également, de manière plus générale, l'avis n° 69.381/4, pp. 67 et 68.

[11] Cette disposition énonce : « Par dérogation à l'alinéa 2, une demande d'une autorité d'obtenir d'un opérateur des adresses IP attribuées à la source d'une connexion n'est autorisée qu'aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique, lorsque cette autorité serait en mesure, à l'aide des informations en sa possession et des adresses IP attribuées à la source de la connexion obtenues de l'opérateur, de tracer le parcours de navigation d'un utilisateur final sur Internet ».

[12] Voir les considérants B.8.4.1 à B.8.4.4.

‡LW-AGFWNFIFE-HBBIEUQ‡

Enfin, il va de soi qu'à défaut de confirmation dans le délai imposé, les arrêtés concernés doivent être réputés n'avoir jamais produit d'effets [13].

L'article 126, § 1er, alinéa 1er, 17°, en projet et, le cas échéant, sa justification seront revus à la lumière de cette observation.

La même observation vaut *mutatis mutandis* en ce qui concerne l'article 126/2, § 2, alinéa 1er, 12°, et l'article 127, § 5, alinéa 1er, 32°, en projet.

3. L'article 126, § 1er, alinéa 3, 2°, entend habiliter le Roi à « fixe[r] les exigences auxquelles ces données doivent répondre ».

Il convient de préciser, dans la justification de l'amendement, ce qu'il faut entendre par le mot « exigences » de manière à déterminer explicitement et sans ambiguïté l'objet de cette habilitation, conformément à ce que requiert l'article 22 de la Constitution.

La même observation vaut en ce qui concerne l'article 126/2, § 4, en projet.

4. À l'article 126, § 2, alinéa 5, les mots « alinéa 2 » seront remplacés par les mots « alinéa 3 ».

Amendement n° 3
Article 126/2 en projet de la loi du 13 juin 2005

1. L'amendement n° 3 entend déterminer, à l'article 126/2, § 2, en projet, les données que les opérateurs offrant aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, doivent conserver pour les zones géographiques visées à l'article 126/1, § 3, en projet [14].

S'agissant de la donnée reprise à l'article 126/2, § 2, alinéa 1er, 7° en projet [15], la justification de l'amendement explique ce qui suit :

> « Elle précise les données de localisation à conserver dans le cadre d'une communication (tout appel ou SMS ou autre type de message entrant ou sortant). Dans le cadre du service d'accès à internet, la communication est toute donnée reçue par l'utilisateur final (ex. toute information reçue dès que la 4G est activée) ou information envoyée (par exemple visite d'un site internet) ».

[13] Voir l'avis n° 68.936/AG, donné le 7 avril 2021 sur un avant-projet devenu la loi du 14 aout 2021 'relative aux mesures de police administrative lors d'une situation d'urgence épidémique', *Doc. parl.*, Chambre, 2020-2021, n° 55-1951/1, pp. 55 à 127, http://www.raadvst-consetat.be/dbx/avis/68936.pdf, observation n° 102.

[14] La plupart de ces données sont énoncées aux paragraphes 2 des articles 3 à 6 de l'arrêté royal du 19 septembre 2013.

[15] À savoir, « [l]es données permettant d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau, qui ont été utilisé(e)s pour effectuer la communication, du début jusqu'à la fin de la communication, ainsi que les dates et heures précises de ces différentes localisations ».

‡LW-AGFWNFIFE-HBBIEUQ‡

Cette explication ne permet pas de comprendre quels sont les éléments permettant de s'assurer que la conservation de cette donnée se concilie avec les réserves que l'Autorité de protection des données a émises dans son avis n° 108/2021 selon lesquelles « la conservation des données de trafic ne doit pas contenir ou permettre de déduire l'url spécifique des pages web visitées par les personnes concernées » [16].

La justification de l'amendement sera complétée en conséquence.

2. Ainsi que le relève l'Autorité de protection des données [17], l'auteur de l'amendement ne justifie pas à suffisance la nécessité et le caractère rigoureusement proportionné de l'obligation de conserver les données visées à l'article 126/2, § 2, alinéa 1er, 9° et 10°, en projet au regard des finalités de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique visées à l'article 126/1, § 1er, alinéa 3, en projet [18].

La justification de l'amendement sera complétée en conséquence.

3. L'article 126/2, § 2, alinéa 1er, 11°, en projet, impose aux opérateurs,

« lorsqu'une donnée précitée n'est pas disponible, [de conserver] toute donnée ayant une fonction équivalente ».

Comme l'explique la justification de l'amendement, l'évolution technologique ainsi que la variété des caractéristiques techniques des services visés par l'obligation de conservation peuvent avoir pour effet de rendre difficile de prévoir l'ensemble des données concernées par cette obligation.

---

[16] Voir le considérant 114 de l'avis n° 108/2021. L'auteur de l'amendement a d'ailleurs suivi ces observations en ce qui concerne les données visées à l'article 126/2, § 2, alinéa 1er, 3°, en projet (« pour les services de communications électroniques à l'exception des services d'accès à Internet, l'adresse IP utilisée par le destinataire de la communication, l'horodatage ainsi que, en cas d'utilisation partagée d'une adresse IP du destinataire, les ports qui lui ont été attribués ») au motif que : « Cette donnée est conservée pour ce qui concerne les services de communications électroniques autres que les services d'accès à internet. En effet, comme l'a rappelé l'Autorité de protection des données dans son avis n° 108/2021 du 28 juin 2021, la conservation des données de trafic ne doit pas contenir ou permettre de déduire l'URL spécifique des pages web visitées par les personnes concernées. Pour ce motif, la conservation de l'adresse IP de destination est exclue pour les services d'accès à internet ».

[17] Voir le considérant 35 de l'avis n° 66/2022 du 1er avril 2022 de l'Autorité de protection des données.

[18] Voir le considérant 11 de la directive 2002/58/CE, qui précise : « À l'instar de la directive 95/46/CE, la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sureté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sureté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ».

‡LW-AGFWNFIFE-HBBIEUQ‡

Toutefois, eu égard à l'ingérence grave dans les droits des personnes concernées qu'emporte une telle obligation – par ailleurs pénalement sanctionnée [19] – de conservation de données qui repose sur les opérateurs, il y a lieu de préciser dans la loi, de manière exhaustive et prévisible, les données pouvant être récoltées dans ce cadre .

Afin de concilier ces impératifs, une solution pourrait être d'habiliter le Roi à déterminer les catégories de données sur lesquelles pourrait porter l'article 126/2, § 2, alinéa 1er, 11°, en projet, en tant qu'elles ont « une fonction équivalente » au regard de l'évolution technologique et des différences techniques entre les divers services visés, pour autant qu'il soit acquis que le respect de la procédure parlementaire ne permet pas au législateur de déterminer ces données et à la condition que l'arrêté royal fasse l'objet d'une confirmation par une loi dans un délai relativement court.

L'article 126/2, § 2, alinéa 1er, 11°, en projet sera revu à la lumière de cette observation.

4. À l'article 126/2, § 2, alinéa 2, en projet, il convient de faire référence à l'arrêté royal « visé à l'alinéa 1er, 12° » [20].

Amendement n° 6

Article 127 en projet de la loi du 13 juin 2005

1. La mention d'un « § 2. » manque dans le dispositif de l'amendement.

2. Il découle de la phrase introductive de l'article 127, § 1er, alinéa 6, en projet qu'il peut être fait usage de toutes les méthodes d'identification indirecte pour les services énumérés au 1° à 3° de cet alinéa.

La section de législation n'aperçoit dès lors pas comment cette phrase introductive se concilie avec le 2° de ce même alinéa qui vise l'hypothèse spécifique dans laquelle l'opérateur « met en œuvre la méthode d'identification indirecte visée au paragraphe 9, alinéa 1er, 4° ».

La rédaction de l'article 127, § 1er, alinéa 6, 2°, en projet sera revue.

3. À l'article 127, § 1er, alinéa 6, 3°, en projet, la référence à l'article 127, § 5, « alinéa 2 » en projet sera remplacée par une référence à l'alinéa 1er de cette disposition.

[19] Voir l'article 145, §1er, en projet (amendement n°8).

[20] Si l'auteur de l'amendement donne suite à la suggestion reprise à l'observation n° 3, il sera, le cas échéant, également fait référence à l'arrêté royal visé au 11°.

‡LW-AGFWNFIFE-HBBIEUQ‡

4.1. L'article 127, § 4, alinéas 3 à 7, en projet énonce :

« Afin d'assurer cette fiabilité et après autorisation du ministre et du ministre de la Justice, l'opérateur ou le point de vente de services de communications électroniques peut réaliser, avec le consentement de l'abonné et de manière automatique, une comparaison entre les paramètres biométriques sur la photo du document d'identité de l'abonné et ceux de son visage.

L'autorisation est accordée à un opérateur ou à une entreprise qui propose la méthode de comparaison visée à l'alinéa 3.

L'autorisation visée à l'alinéa 3 a pour objectif de vérifier la fiabilité de cette comparaison pour les besoins des autorités.

L'opérateur offre à l'abonné au moins une manière alternative de s'identifier.

L'opérateur et le point de vente ne peuvent communiquer ces paramètres biométriques à un tiers au sens de l'article 4, 10) du RGPD. Ils ne peuvent les traiter que dans les limites nécessaires en vue d'accomplir la finalité de comparaison faciale visée à l'alinéa 3 ».

Cette disposition autorise l'opérateur ou le point de vente à comparer les paramètres biométriques repris sur la photo du document d'identité de l'abonné avec ceux de son visage.

Cette disposition appelle les observations suivantes.

4.2. Tout traitement de données à caractère personnel doit, entre autres, respecter les exigences générales reprises à l'article 5, paragraphe 1, du RGPD.

Parmi ces exigences se trouve le principe de minimisation des données qui requiert que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

S'agissant de la méthode d'identification en cause, qui repose sur le traitement de données biométriques, les justifications reprises dans la justification de l'amendement ne sont pas convaincantes [21].

Il appartient dès lors à l'auteur de l'amendement de préciser, dans la justification de celui-ci, les éléments qui permettent de considérer que le principe de minimisation des données est effectivement respecté en l'espèce, alors que d'autres moyens, moins intrusifs au regard de la vie privée, existent et apparaissent être suffisants pour démontrer l'identité de l'abonné, même pour ceux qui ne peuvent avoir recours à l'eID ou à des prestataires de services de confiance qualifiés qui offrent un service de signature électronique qualifiée [22].

4.3. Conformément à l'article 9, paragraphe 1, du RGPD, le traitement des données biométriques aux fins d'identifier une personne physique de manière unique porte sur des données sensibles et est, en principe, interdit.

[21] Voir, les considérants 51 à 54 de l'avis n° 66/2022 de l'Autorité de protection des données.

[22] Comme, par exemple, se rendre physiquement au point de vente.

‡LW-AGFWNFIFE-HBBIEUQ‡

Ce n'est que dans le cas où l'une des conditions visées à l'article 9, paragraphe 2, du RGPD est remplie qu'un tel traitement serait admissible, sous réserve du respect des exigences générales de ce même règlement.

En l'occurrence, l'article 9, paragraphe 2, a), du RGPD autorise un tel traitement si

> « la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée ».

Afin de répondre aux exigences résultant de cette disposition, il y a lieu de revoir l'article 127, § 4, alinéas 3 à 8 en manière telle qu'il soit précisé que le consentement explicite de l'abonné sera recueilli, étant entendu que la manifestation de volonté de l'abonné doit, conformément à l'article 7 du RGPD, combiné avec son article 4, 11), être libre, spécifique, éclairée et univoque, ce qui implique que l'abonné soit informé des finalités pour lesquelles ces données seront récoltées et que la méthode alternative d'identification proposée ne peut être à ce point contraignante que l'abonné n'aura d'autre choix que d'autoriser le traitement de ses données biométriques.

Enfin, la disposition en projet précisera, comme cela ressort de la justification de l'amendement, que les données biométriques ne seront pas conservées une fois la comparaison en question effectuée.

L'article 127, § 4, alinéas 3 à 8, en projet sera revu à la lumière de cette observation.

4.4. Les ministres concernés sont appelés, conformément à l'article 127, § 4, alinéa 3, en projet, à autoriser la comparaison des données biométriques des abonnés avec celles de leur visage.

La disposition en projet ne fixe aucun critère qui délimiterait leur pouvoir d'appréciation sur ce point en vue d'octroyer les autorisations considérées.

Le principe de légalité inscrit à l'article 22 de la Constitution et la sécurité juridique imposent que ces critères soient, en leurs éléments essentiels, fixés par le législateur.

La disposition en projet sera revue en ce sens.

5. Aux fins de garantir le respect des principes d'intégrité et de confidentialité des documents d'identification, qui découlent de l'article 5 du RGPD, il conviendrait, à l'article 127, § 5, alinéa 3, en projet de prévoir que ces documents ne peuvent être copiés que dans la mesure où il n'est pas possible d'extraire de manière électronique et sécurisée les données d'identification et pour autant que des mesures techniques soient prises par les opérateurs pour éviter toute reproduction conforme du document d'identité copié [23].

[23] Voir, en ce sens, la note de bas de page n° 43 de l'avis n° 66/2022 de l'Autorité de protection des données.

‡LW-AGFWNFIFE-HBBIEUQ‡

La même observation vaut *mutatis mutandis* en ce qui concerne l'obligation similaire qui pèse sur les personnes morales à l'article 127, § 10, alinéa 2, 4°, en projet.

6. L'article 127, § 5, alinéas 4 et 5, en projet énonce :

> « Lorsque l'abonné soumet un document d'identification visé à l'alinéa 1er pour s'identifier et que l'opérateur n'est pas en mesure d'assurer la fiabilité de l'identité de l'abonné sur base de ce document, il peut demander à l'abonné, afin de renforcer cette fiabilité, de lui communiquer :
>
> – des factures de fournisseurs de différents produits ou services, pour les services de communications électroniques qui sont payés après leur fourniture ;
>
> – des informations complémentaires.
>
> L'opérateur conserve une copie de ces factures et de ces informations ».

Cette disposition ne répond pas aux exigences de prévisibilité applicables en matière de droit à la vie privée dans la mesure où les factures et informations complémentaires ne sont pas suffisamment précisées et pourraient dès lors se rapporter à n'importe quelle information relative à un abonné, ce qui n'apparait pas admissible.

Par ailleurs, la section de législation n'aperçoit, sur la base des informations dont elle dispose, ni la pertinence ni la proportionnalité d'une telle mesure pour les besoins d'identification de l'abonné.

L'article 127, § 5, alinéas 4 et 5, en projet sera réexaminé à la lumière de cette observation.

7. L'article 127, § 5, alinéa 6, en projet énonce :

> « Le Roi peut autoriser certaines méthodes d'identification spécifiques, le cas échéant indirectes, pour les personnes qui ne disposent d'aucun des documents visés à l'alinéa 1er ».

Si cette habilitation doit effectivement être comprise comme autorisant le Roi à déterminer des données et documents d'identification qui ne sont pas prévus à l'article 127 [24] en projet, la délégation ainsi prévue contrevient à l'article 22 de la Constitution, tel qu'interprété par la Cour constitutionnelle, qui exige que ces éléments essentiels soient repris dans une loi formelle [25].

Une telle habilitation ne serait admissible que si l'arrêté royal en question devait être confirmé par une loi dans un délai relativement court et à la condition que l'auteur de l'amendement soit en mesure d'établir que le respect de la procédure parlementaire ne permet pas au législateur de déterminer les données et documents d'identification en question en temps utile.

[24] C'est ce qui parait ressortir notamment de l'article 127, § 6, qui énonce : « Sans préjudice des données conservées sur base de l'arrêté royal pris le cas échéant en exécution du paragraphe 5, alinéa [6] ».

[25] L'avant-projet justifie cette habilitation comme suit : « La possibilité est laissée au Roi de trouver des solutions ad hoc créatives pour les personnes qui ne disposeraient d'aucun des documents d'identité mentionnés dans l'article 127 ».

‡LW-AGFWNFIFE-HBBIEUQ‡

La disposition à l'examen et, le cas échéant, sa justification seront revues à la lumière de la présente observation.

La même observation vaut *mutatis mutandis* en ce qui concerne les habilitations contenues à l'article 127, § 6, alinéa 2, 2ème tiret et à l'article 127, § 9, 5°, en projet.

8. L'article 127, § 6, détermine, à l'alinéa 1er, la liste de données d'identification que l'opérateur doit « au maximum » conserver ainsi que, à l'alinéa 2, la liste de données d'identification que l'opérateur doit « au minimum » conserver.

De deux choses l'une.

Soit, seules les données reprises à l'alinéa 2 sont nécessaires et suffisantes au regard des finalité d'identification de l'utilisateur puisqu'il s'agit des données que les opérateurs doivent « au minimum » conserver. Dans ce cas de figure, il n'y a pas lieu d'exiger que les données reprises à l'alinéa 1er soient également conservées.

Soit les données reprises à l'alinéa 1er sont également nécessaires au regard de cette finalité, en ce sens qu'elles permettent de s'assurer, dans le respect du principe de minimisation, de l'identité de l'utilisateur étant entendu qu'il n'est pas toujours possible pour les opérateurs de récolter ces données pour l'ensemble des utilisateurs concernés. Dans ce dernier cas de figure, la rédaction de l'article 127, § 6, en projet sera revue afin de mieux faire ressortir la manière dont s'articulent les deux listes de données, notamment en ne mentionnant pas à l'alinéa 1er les données devant déjà être conservées conformément à l'alinéa 2.

L'article 127, § 6, en projet et sa justification seront revus à la lumière de cette observation.

9. L'article 127, § 6, alinéa 1er, 5°, en projet énonce :

> « Sans préjudice des données conservées sur base de l'arrêté royal pris le cas échéant en exécution du paragraphe 5, alinéa [6], lorsqu'un opérateur identifie l'abonné qui est une personne physique par le biais d'une méthode d'identification directe, il conserve au maximum les données d'identification suivantes :
>
> […]
>
> 5° la photo de l'abonné mais uniquement pour les documents d'identité autres que la carte d'identité électronique belge ».

La conservation d'une photographie en vue de l'identification d'une personne – telle qu'elle est prévue par le dispositif à l'examen – doit être considérée comme le traitement d'une donnée biométrique [26], ce qui implique qu'une des hypothèses prévues à l'article 9, paragraphe 2, du RGPD doit être rencontrée pour pouvoir procéder à un tel traitement.

[26] Voir, en ce sens, le considérant n° 51 du RGPD : « le traitement des photographies ne devrait pas systématiquement être considéré comme constituant un traitement de catégories particulières de données à caractère personnel, étant donné que celles-ci ne relèvent de la définition de données biométriques que lorsqu'elles sont traitées selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique. De telles données à caractère personnel ne devraient pas faire l'objet d'un traitement, à moins que celui-ci ne soit autorisé dans

‡LW-AGFWNFIFE-HBBIEUQ‡

L'article 9, paragraphe 2, g), du RGPD semble pouvoir constituer la base sur laquelle la photo en question pourrait être conservée.

Cette disposition énonce :

> « [L]e traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ».

Il appartient à l'auteur de l'amendement d'être en mesure de justifier que les exigences imposées par cette disposition sont rencontrées en l'espèce.

La disposition sera revue à la lumière de cette observation. Le cas échéant, la justification de l'amendement sera complétée en conséquence.

10. À l'article 127, § 6, alinéa 1er, 8°, en projet, il convient, à tout le moins dans la justification de l'amendement, de préciser ce qu'il y a lieu d'entendre par « numéro de sécurité publique ».

11. L'auteur de l'amendement doit être en mesure de justifier l'obligation de récolter et conserver, conformément à l'article 127, § 9, 3°, en projet, la date et le lieu de naissance de l'abonné lorsqu'il effectue un paiement électronique alors que la référence de l'opération ainsi que le nom et le prénom de l'abonné paraissent suffisants pour pouvoir l'identifier [27].

12. L'article 127, § 10, alinéa 5, en projet énonce :

> « L'opérateur conserve le numéro de châssis du véhicule dans lequel une de ses cartes SIM (« *subscriber identity/identification module* ») ou toute carte équivalente a été intégrée, ainsi que lien entre le numéro de châssis et le numéro de cette carte, à partir de la date d'activation du service de communications électroniques jusqu'à douze mois après la fin du service ».

Le numéro d'identification d'un véhicule peut donner accès à de nombreuses informations sur le véhicule concerné et, de manière indirecte, sur son propriétaire [28].

Eu égard à la finalité de l'identification du propriétaire du véhicule, il convient de prévoir que seule cette dernière information pourra être communiquée aux autorités dans le cadre de leurs missions.

---

des cas spécifiques prévus par le présent règlement, compte tenu du fait que le droit d'un État membre peut prévoir des dispositions spécifiques relatives à la protection des données visant à adapter l'application des règles du présent règlement en vue de respecter une obligation légale ou pour l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ».

[27] Voir, en ce sens, le considérant n° 76 de l'avis n° 66/2022 de l'Autorité de protection des données.

[28] Voir l'article 18 de la loi du 19 mai 2010 'portant création de la Banque-Carrefour des véhicules' et l'article 2 de l'arrêté royal du 8 juillet 2013 portant exécution de la loi du 19 mai 2010 portant création de la Banque-Carrefour des Véhicules'.

‡LW-AGFWNFIFE-HBBIEUQ‡

L'article 127, § 10, alinéa 5, en projet et sa justification seront revus à la lumière de cette observation.

Amendement n° 9
Article 40 du projet de loi

La justification de l'article 40 que l'amendement n° 9 entend insérer dans le projet de loi explique que l'article 127 en projet ne s'appliquera « que pour les contrats postérieurs à l'entrée en vigueur de la loi ».

L'article 40 du projet de loi gagnerait à reproduire explicitement cette modalité d'entrée en vigueur qui ne ressort pas clairement du dispositif en projet.

Par ailleurs, la justification de l'amendement sera complétée de manière à préciser ce qu'il convient d'entendre par les termes « contrats postérieurs ». Ce manque de précision pourrait en effet susciter des difficultés en pratique, eu égard à la multitude de services complémentaires pouvant être offerts, gratuitement ou non, à des personnes bénéficiant déjà d'un contrat en cours avec un opérateur [29].

L'article 40 du projet de loi et sa justification seront revus à la lumière de cette observation.

Amendement n° 12
Article 15 en projet de la loi du 17 janvier 2003

1. L'article 15, §§ 1er et 2 en projet, de la loi du 17 janvier 2003 'relative au statut du régulateur des secteurs des postes et des télécommunications belges' entend permettre à l'Institut belge des postes et des télécommunications (ci-après : l'IBPT) , lorsque c'est nécessaire pour lui permettre « d'accomplir l'une de ses missions d'application et de contrôle des dispositions énumérées à l'article 14, paragraphe 1er, 3°, a) et g) à i), », d'accéder aux « données relatives à l'abonné ou à l'utilisateur habituel du service » [30] et aux « métadonnées de communications électroniques » [31] autres que les données relatives à l'abonné ou à l'utilisateur habituel du service.

[29] Voir, à cet égard, l'article 127, § 2, alinéa 1er, 1°, en projet qui définit ainsi le service de communications électroniques payant comme étant le « service de communications électroniques pour lequel un paiement de l'abonné à l'opérateur est nécessaire pour utiliser le service ou continuer à l'utiliser, ainsi que tout service de communications électroniques offert sans surcout par l'opérateur à l'abonné conjointement à ce service ».

[30] Ces données sont, conformément à l'article 2, 5°, en projet de la loi du 17 janvier 2003 (amendement n° 10), « les données relatives à l'abonné ou à l'utilisateur habituel du service de communications électroniques, – visées aux articles 126 et 127 de la loi du 13 juin 2005 relative aux communications électroniques, ou ; – conservées en vertu de l'article 122 de la loi du 13 juin 2005 relative aux communications électroniques et qui permettent d'identifier l'abonné ou l'utilisateur habituel du service ».

[31] L'article 2, 93°, en projet de la loi du 13 juin 2005 définit les métadonnées de communications électroniques comme suit : « les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de

‡LW-AGFWNFIFE-HBBIEUQ‡

Comme l'indique la justification de l'amendement, l'IBPT doit avoir accès à ces données au regard des finalités suivantes :

> « Les paragraphes 1 et 2 visent les missions d'application et de contrôle du respect de la loi télécom (art. 14, § 1er, 3°, a)) et des autres législations sectorielles en matière de sécurité des réseaux et des systèmes d'information (à savoir : art. 14, § 1er, 3°, g) la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ; h) la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne le secteur des infrastructures numériques ; et i) le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques).
>
> Les finalités poursuivies par ces paragraphes correspondent aux finalités suivantes prévues à l'article 127/1, § 2, de la loi télécom :
>
> – la prévention de menaces graves contre la sécurité publique (art. 127[/1], § 2, 2° de la loi télécom) ;
>
> – l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques (art. 127[/1], § 2, 4° de la télécom) ;
>
> – le contrôle de la loi télécom par l'Institut et les missions de contrôle des autorités compétentes pour la protection des données dans le cadre de leurs missions de contrôle (art. 127[/1], § 2, 9° de la loi télécom) ».

L'IBPT pourrait ainsi avoir accès à l'ensemble des données énumérées, sans qu'une distinction soit opérée entre les catégories de données en fonction de la finalité précise qui justifie l'accès à ces données [32].

La question se pose de savoir s'il est nécessaire que l'IBPT ait accès à l'ensemble de ces données au regard des différentes missions qui lui sont ainsi attribuées.

Il en va à fortiori ainsi en ce qui concerne l'accès aux métadonnées de communications électroniques qui comprennent, sans s'y limiter, les données prévues à l'article 126/2 en projet, soit des données de trafic et de localisation de toutes les communications effectuées à partir ou vers une des zones géographiques qu'il liste, et donc des données particulièrement intrusives dans la vie privée des utilisateurs.

La justification de l'amendement n'est pas suffisamment éclairante à cet égard.

‡LW-AGFWNFIFE-HBBIEUQ‡

l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication ».

[32] Voir, en ce sens, l'avis n° 69.381/4.

Il appartient à l'auteur de l'amendement d'être en mesure d'établir les éléments qui permettent de justifier la nécessité et le caractère proportionné de la possibilité d'accéder à l'ensemble de ces données (ou une partie d'entre elles), et ce mission par mission dans le respect de la jurisprudence de la Cour de justice [33].

La justification de l'amendement sera utilement complétée à cet égard.

La même observation vaut *mutatis mutandis* en ce qui concerne l'amendement n° 15 qui entend autoriser, à l'article 25/1 en projet de la loi du 17 janvier 2003, les officiers de police judiciaire de l'IBPT à accéder aux mêmes données afin de rechercher, de constater ou de poursuivre une infraction visée à l'article 145, § 3 ou § 3*bis*, de la loi du 13 juin 2005 ou à l'article 24, § 1er, 2°, de la loi du 17 janvier 2003.

2. La Cour de justice exige qu'afin de garantir, en pratique, le plein respect des critères objectifs définissant les circonstances et les conditions auxquelles l'accès aux données relatives au trafic et à des données de localisation est accordé aux autorités nationales compétentes, il est essentiel que cet accès soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités [34].

Par ailleurs, la Cour constitutionnelle a souligné qu'un tel contrôle préalable n'est pas exigé pour une demande d'accès à des données d'identification, contrairement à une demande d'accès portant sur des données relatives au trafic et à des données de localisation [35].

Il convient donc de s'assurer que les « données relatives à l'abonné ou à l'utilisateur habituel du service » définies à l'article 2, 5°, en projet de la loi du 17 janvier 2003, auxquelles l'IBPT peut accéder conformément à l'article 15, § 1er, en projet, ne comprennent que des données d'identification, à défaut de quoi un contrôle préalable externe devra être mis en place pour pouvoir accéder aux autres données.

La justification de l'amendement sera complétée en conséquence.

La même observation vaut *mutatis mutandis* pour l'article 25/1, § 1er, 1°, en projet de la loi du 17 janvier 2003 (amendement n° 15).

Amendement n° 15
Article 25/1 en projet de la loi du 17 janvier 2003

À l'article 25/1, § 4, alinéas 1er et 3 en projet de la loi du 17 janvier 2003, les mots « en temps réel » seront remplacés par les mots « sans délai ».

[33] Voir, en ce sens, les considérants 89 à 103 de l'avis n° 66/2022 de l'Autorité de protection des données.

[34] Considérants 50 et 51 de l'arrêt C-746/18 du 2 mars 2021.

[35] Considérant B.16.8.6 de l'arrêt n° 158/2021 du 18 novembre 2021.

‡LW-AGFWNFIFE-HBBIEUQ‡

En effet, la notion de « temps réel » peut prêter à confusion dès lors qu'elle peut revêtir une signification particulière dans le cadre de traitements de données dans le domaine des communications électroniques [36].

La même observation vaut pour les article 46*bis*, §§ 3 et 4, alinéa 2, en projet du Code d'instruction criminelle (amendement n° 16).

Amendement n° 17
Article 11 en projet de la loi du 24 janvier 1977

Il convient de préciser, à l'article 11, § 1er, alinéa 11, en projet, de la loi du 24 janvier 1977 'relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits', que la transaction bancaire doit avoir été préalablement communiquée par un opérateur conformément aux conditions fixées par la loi du 13 juin 2005.

*

[36] Voir, à titre d'illustration, les considérants 183 et suivants de l'arrêt *La Quadrature du Net*.

‡LW-AGFWNFIFE-HBBIEUQ‡

Aangezien de adviesaanvraag ingediend is op basis van artikel 84, § 1, eerste lid, 2°, van de wetten 'op de Raad van State', gecoördineerd op 12 januari 1973, beperkt de afdeling Wetgeving overeenkomstig artikel 84, § 3, van de voornoemde gecoördineerde wetten haar onderzoek tot de rechtsgrond van het voorontwerp,‡ de bevoegdheid van de steller van de handeling en de te vervullen voorafgaande vormvereisten.

Wat die drie punten betreft, geven de amendementen aanleiding tot de volgende opmerkingen.

VOORAFGAANDE OPMERKING

Gelet op het grote aantal dossiers die momenteel zijn voorgelegd aan het advies van de afdeling Wetgeving van de Raad van State en op de inhoud van de amendementen, alsook op het zeer technische karakter van een aantal van de onderzochte bepalingen, kon de afdeling Wetgeving geen exhaustief onderzoek van de amendementen verrichten, ook al beperkt dat onderzoek zich tot de drie punten die worden vermeld in artikel 84, § 3, eerste lid, van de 'wetten op de Raad van State', gecoördineerd op 12 januari 1973.

Voor alle aspecten die niet onder het voorliggende advies vallen, verwijst de afdeling Wetgeving naar haar advies nr. 69.381/4, gegeven op 28 juni 2021 over het voorontwerp, dat heeft geleid tot het wetsontwerp 'betreffende het verzamelen en het bewaren van de identificatie-, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten'[1] (hierna : "het wetsontwerp"), waarin verscheidene voorliggende amendementen wijzigingen beogen aan te brengen.

Tot slot wijst de afdeling Wetgeving erop dat haar adiëring per definitie beperkt is tot de ontworpen teksten en dat het haar gelet op het voorgaande niet toekomt te onderzoeken of het geheel van het Belgisch positief recht het recht op eerbiediging van het privéleven kan waarborgen bij het verzamelen en het gebruiken van de gegevens waarvan dit ontwerp de bewaring regelt. Aldus hangt de vraag of de aaneenschakeling van de verzameling van, de bewaring van, de toegang tot en het gebruik van de betrokken gegevens verenigbaar is met de fundamentele rechten en vrijheden in kwestie af van andere geldende bepalingen, ongeacht of ze al dan niet een algemene strekking hebben, die in de voorliggende adviesaanvraag niet aan de afdeling Wetgeving zijn voorgelegd.

Het spreekt vanzelf dat in de zonet genoemde omstandigheden niets mag worden afgeleid uit het feit dat in dit advies geen opmerkingen zijn geformuleerd over sommige bepalingen of sommige kwesties.

‡ Aangezien het gaat om amendementen op een ontwerp van wet wordt onder "rechtsgrond" de overeenstemming met de hogere rechtsnormen verstaan.

[1] *(Parl.St.* Kamer 2021-22, nr.55-2572/1, 219 tot 320, (http://www.raadvst-consetat.be/dbx/adviezen/69381.pdf). Het voorontwerp werd bij de Kamer van volksvertegenwoordigers ingediend op 17 maart 2022.

‡LW-AGFWNFIFE-HBBIEUQ‡

STREKKING VAN DE AMENDEMENTEN[2]

I. Jurisprudentiële context

A. De arresten van het Hof van Justitie van de Europese Unie

1. In een arrest C-207/16 van 2 oktober 2018[3] heeft het Hof van Justitie van de Europese Unie (hierna: het Hof van Justitie) voor recht gezegd dat "artikel 15, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 'betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie)', aldus moet worden uitgelegd dat de toegang van overheidsinstanties tot de identificatiegegevens van houders van met een gestolen mobiele telefoon geactiveerde simkaarten – zoals hun naam, voornaam en, in voorkomend geval, adres – geen zodanig ernstige inmenging in de door die artikelen van het Handvest gewaarborgde grondrechten van laatstgenoemden oplevert dat die toegang – op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten – moet worden beperkt tot de bestrijding van zware criminaliteit.

2. Bij een arrest C-511/18 van 6 oktober 2020[4,] heeft het Hof van Justitie voor recht verklaard dat artikel 15, lid 1, van richtlijn 2002/58/EG aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die, voor de in dat artikel 15, lid 1, genoemde doeleinden, preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens.

Artikel 15, lid 1, van richtlijn 2002/58/EG verzet zich daarentegen niet tegen wettelijke maatregelen

– die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische[-]communicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

[2] De adviesaanvrager heeft de drie laatste amendementen niet genummerd. Ten behoeve van het voorliggende advies moeten ze, volgend op de andere amendementen, worden genummerd als de amendementen 16, 17 en 18.

[3] HvJ (grote kamer), arrest *Ministerio Fiscal*, 2 okotober 2018, C-207/16, ECLI:EU:C:2018:788.

[4] HvJ (grote kamer), arrest *La Quadrature du Net e.a.*, 6 oktober 2020, C-511/18, ECLI:EU:C:2020:791.

‡LW-AGFWNFIFE-HBBIEUQ‡

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

– die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische[-]communicatiemiddelen, en

– die het mogelijk maakt om ten behoeve van de bestrijding van zware criminaliteit en, *a fortiori*, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronische[-]communicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik;

3. Ten slotte heeft het Hof van Justitie in een arrest C-746/18 van 2 maart 2021,[5] voor recht verklaard dat:

– artikel 15, lid 1, van richtlijn 2002/58/EG aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die de mogelijkheid biedt om overheidsinstanties met het oog op het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten toegang te verlenen tot een reeks verkeers- of locatiegegevens die informatie kunnen verschaffen over de communicaties van een gebruiker van een elektronische[-] communicatiemiddel of over de locatie van de door hem gebruikte eindapparatuur en waaruit precieze conclusies kunnen worden getrokken over zijn persoonlijke levenssfeer, welke toegang niet beperkt is tot procedures ter bestrijding van zware criminaliteit en ter voorkoming van ernstige bedreigingen van de openbare veiligheid, en dit ongeacht de duur van de periode waarvoor om toegang tot dergelijke gegevens wordt verzocht en ongeacht de hoeveelheid en de aard van de gegevens die voor die periode beschikbaar zijn;

[5] HvJ (grote kamer) arrest *Prokuratuur*, 2 maart 2021, C-746/18, ECLI:EU:C:2021:152. Zie eveneens HvJ (grote kamer), arrest *G.D.*, 5 april 2022, C-140/20, ECLI:EU:C:2022:258.

‡LW-AGFWNFIFE-HBBIEUQ‡

– artikel 15, lid 1, van richtlijn 2002/58/EG aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die het openbaar ministerie, dat tot taak heeft de strafprocedure in te leiden en, in voorkomend geval, in een latere procedure op te treden als openbaar aanklager, de bevoegdheid toekent om een overheidsinstantie ten behoeve van een strafrechtelijk onderzoek toegang te verlenen tot verkeers- en locatiegegevens.

B. De arresten van het Grondwettelijk Hof

4. Naar aanleiding van de voormelde arresten van het Hof van Justitie heeft het Grondwettelijk Hof op 22 april 2021 arrest nr. 57/2021 gewezen met de volgende motivering:

> "B.15. Uit het voormelde arrest van het Hof van Justitie van 6 oktober 2020 in zake *La Quadrature du Net e.a.*, blijkt dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in dat artikel 15, § 1, genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, behalve in de in het voormelde arrest beschreven beperkte gevallen.
>
> In zoverre zij principieel en zonder beperking tot die gevallen voorziet in een algemene en ongedifferentieerde bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de identificatiegegevens, de toegangs- en verbindingsgegevens, alsook van de communicatiegegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005 ['betreffende de elektronische communicatie'], schendt de bestreden wet bijgevolg artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de voormelde bepalingen van het Handvest van de grondrechten van de Europese Unie, en in samenhang met de artikelen 10 en 11 van de Grondwet.
>
> B.16.1. In het dictum van het voormelde arrest van 6 oktober 2020, in zake *La Quadrature du Net e.a.*, preciseert het Hof van Justitie echter dat artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8 en 11 alsook van artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, zich niet verzet tegen verschillende soorten wettelijke maatregelen die het Hof opsomt. Toelaatbaar zijn aldus, met name, wettelijke maatregelen "die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk", of nog wettelijke maatregelen "die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen". Die wettelijke maatregelen moeten, "door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik".

‡LW-AGFWNFIFE-HBBIEUQ‡

B.16.2. Op grond van die preciseringen van het Hof van Justitie betoogt de Ministerraad in zijn aanvullende memories dat de bestreden wet in elk geval niet dient te worden vernietigd in zoverre zij voorziet in de algemene en ongedifferentieerde verplichting tot bewaring, door de operatoren en aanbieders van elektronische communicatiediensten, van de IP-adressen die zijn toegewezen aan de bron van een verbinding, enerzijds, en van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen, anderzijds.

De Ministerraad besluit daaruit dat, in voorkomend geval, enkel het tweede en het derde lid van artikel 126, § 3, van de wet van 13 juni 2005 dienen te worden vernietigd, waarin respectievelijk de verbindings- en locatiegegevens en de communicatiegegevens worden beoogd. Hij is van mening dat het eerste lid van het voormelde artikel 126, § 3, waarin de identificatiegegevens worden beoogd, daarentegen niet dient te worden vernietigd, net zomin als de andere bepalingen van de bestreden wet, aangezien zij de nodige waarborgen bevatten op het vlak van bewaring van en toegang tot de gegevens.

B.17. Te dezen dient te worden vastgesteld dat de bestreden wet, wat het beginsel zelf ervan betreft, berust op een verplichting tot algemene en ongedifferentieerde bewaring van alle gegevens beoogd in artikel 126, § 3, van de wet van 13 juni 2005, en dat zij, in het algemeen, zoals in B.3 en B.4 is vermeld, ruimere doelstellingen nastreeft dan de bestrijding van zware criminaliteit of het risico van aantasting van de openbare veiligheid.

Het onderscheid dat bij artikel 126, § 3, van de wet van 13 juni 2005 wordt gemaakt tussen drie categorieën van gegevens (te weten: identificatiegegevens, toegangs- en verbindingsgegevens, alsook communicatiegegevens) heeft slechts een weerslag op het startpunt van de bewaringstermijn van de gegevens - in elk geval twaalf maanden -, en eventueel op de mogelijkheden voor de gemachtigde instanties om toegang tot die gegevens te hebben (zie artikel 46*bis* van het Wetboek van strafvordering en artikel 126, § 2, van de wet van 13 juni 2005). Die categorisering stemt daarenboven niet overeen met het onderscheid dat door het Hof van Justitie in zijn arrest van 6 oktober 2020 wordt gemaakt voor wat betreft de verschillende categorieën van gegevens die het voorwerp kunnen uitmaken van een verplichting tot algemene en ongedifferentieerde bewaring, mits verscheidene voorwaarden in acht worden genomen (te weten, te dezen: de IP-adressen die zijn toegewezen aan de bron van een verbinding en de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronische communicatiemiddelen).

B.18. Bij het arrest van het Hof van Justitie van 6 oktober 2020 wordt een verandering van gezichtspunt opgelegd ten opzichte van de keuze die de wetgever heeft gemaakt: de verplichting tot bewaring van gegevens met betrekking tot elektronische communicatie moet de uitzondering zijn, en niet de regel. De regeling waarbij in een dergelijke verplichting wordt voorzien, moet daarenboven onderworpen zijn aan duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel, waarbij een minimum aan vereisten worden opgelegd (punt 133). Die regeling moet waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt en moet steeds 'beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel' (punten 132 en 133).

‡LW-AGFWNFIFE-HBBIEUQ‡

B.19. Het staat aan de wetgever een regeling tot stand te brengen waarbij de beginselen in acht worden genomen die van toepassing zijn inzake bescherming van persoonsgegevens, in het licht van de rechtspraak van het Hof van Justitie, en, in voorkomend geval, rekening te houden met de door dat Hof aangebrachte preciseringen wat betreft de verschillende soorten wettelijke maatregelen die verenigbaar worden geacht met artikel 15, lid 1, van de richtlijn 2002/58/EG, gelezen in het licht van de artikelen 7, 8, 11 en 52, lid 1, van het Handvest van de grondrechten van de Europese Unie. In het bijzonder staat het, in die context, ook aan de wetgever tussen de verschillende soorten aan bewaring onderworpen gegevens het onderscheid te maken dat geboden is, zodat wordt gewaarborgd dat, voor elk soort gegeven, de inmenging tot het strikt noodzakelijke wordt beperkt.

B.20. Rekening houdend met hetgeen voorafgaat, dienen de artikelen 2, b), 3 tot 11 en 14 van de bestreden wet, die onlosmakelijk met elkaar verbonden zijn, te worden vernietigd."

5. In die context hebben de stellers van het wetsontwerp waarop de amendementen betrekking hebben, derhalve besloten een regeling vast te stellen die tot doel heeft een regeling voor gegevensbewaring in te voeren om de doelstellingen te bereiken die het Hof van Justitie en het Grondwettelijk Hof legitiem hebben geacht en die in overeenstemming is met het dictum en de motivering van de beslissingen van die hoge rechtscolleges, in het bijzonder met de uit die beslissingen voortvloeiende grenzen en criteria inzake het bewaren van verkeers- en locatiegegevens door de operatoren die actief zijn in de sector van de elektronische communicatie alsook inzake de toegang tot die gegevens door de overheden.

6. Bij een arrest nr. 158/2021 van 18 november 2021 heeft het Grondwettelijk Hof artikel 2 van de wet van 1 september 2016 'tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de organieke wet van 30 november 1998 'houdende regeling van de inlichtingen- en veiligheidsdiensten' vernietigd, zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen.

Die vernietigde bepaling luidt als volgt:

"In artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie, gewijzigd bij de wetten van 4 februari 2010, 10 juli 2012, 27 maart 2014 en 29 mei 2016, worden de volgende wijzigingen aangebracht:

1° in paragraaf 1 worden de volgende wijzigingen aangebracht :

(...)

c) tussen het eerste en het tweede lid worden zeven leden ingevoegd, luidende:

'Wat de identificatie van de eindgebruiker betreft, is de operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, verantwoordelijk voor de verwerking in de zin van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

Behoudens tegenbewijs wordt de geïdentificeerde persoon geacht zelf de elektronische-communicatiedienst te gebruiken.

‡LW-AGFWNFIFE-HBBIEUQ‡

Wanneer de eindgebruiker een identificatiedocument voorlegt waarop het rijksregisternummer staat, verzamelt de operator, de aanbieder bedoeld in artikel 126, § 1, eerste lid, het verkoopkanaal van elektronische-communicatiediensten of de onderneming die een identificatiedienst verstrekt, dat nummer.

Het verkoopkanaal van elektronische-communicatiediensten bewaart geen identificatiegegevens of -documenten, die worden overgezonden naar de operator, naar de aanbieder bedoeld in artikel 126, § 1, eerste lid, of naar de onderneming die een identificatiedienst verstrekt.

Indien een rechtstreekse invoer in de computersystemen van de operator, van de aanbieder bedoeld in artikel 126, § 1, eerste lid, of van de onderneming die een identificatiedienst verstrekt, niet mogelijk is, mag het verkoopkanaal van elektronische-communicatiediensten een kopie maken van het identificatiedocument, waaronder van de Belgische elektronische identiteitskaart, maar deze kopie wordt uiterlijk na de activering van de elektronische-communicatiedienst vernietigd.

De operator of de aanbieder bedoeld in artikel 126, § 1, eerste lid, bewaart een kopie van de andere identificatiedocumenten dan de Belgische elektronische identiteitskaart.

De verzamelde identificatiegegevens en -documenten worden bewaard overeenkomstig artikel 126, § 3, eerste lid'.

(...)."

De beslissing van het Grondwettelijk Hof wordt gemotiveerd als volgt:

"Ten aanzien van het eerste middel

(...)

B.8.4.1. Wat de betrokken identificatiegegevens en identificatiedocumenten betreft, bepaalt artikel 127 van de bestreden wet dat het moet gaan om documenten die het rijksregisternummer bevatten, alsook dat het rijksregisternummer een persoonsgegeven is dat in dit verband dient te worden verzameld en verwerkt. De overige identificatiegegevens, alsook de identificatiedocumenten die in aanmerking komen, worden, in weerwil van de in B.8.1 vermelde adviezen, niet in die wetsbepaling opgesomd.

B.8.4.2. Bovendien heeft de wetgever de Koning geen uitdrukkelijke machtiging gegeven om die identificatiegegevens en identificatiedocumenten nader te bepalen. Dergelijke essentiële elementen van een verwerking van persoonsgegevens kunnen nochtans niet worden begrepen onder de vage machtiging in artikel 127, § 1, eerste lid, van de wet van 13 juni 2005 om de nodige "technische en administratieve maatregelen" te nemen met het oog op de identificeerbaarheid van de eindgebruiker.

De Koning diende die identificatiegegevens en -documenten bijgevolg vast te stellen op grond van de bevoegdheid die Hij aan artikel 108 van de Grondwet ontleent om de verordeningen en de besluiten te nemen die voor de uitvoering van de wetten nodig zijn.

Die algemene uitvoeringsbevoegdheid van de Koning kan te dezen evenwel niet volstaan. Een delegatie van essentiële elementen van een door de Grondwetgever aan de formele wetgever voorbehouden aangelegenheid is immers slechts mogelijk indien de inachtneming van de parlementaire procedure de wetgever niet in staat zou stellen een doelstelling van algemeen belang te verwezenlijken, en op voorwaarde dat hij het onderwerp van die machtiging uitdrukkelijk en ondubbelzinnig vaststelt en dat de door de Koning genomen maatregelen door de wetgevende macht worden onderzocht met het oog op hun bekrachtiging binnen een relatief korte termijn, vastgesteld in de machtigingswet.

‡LW-AGFWNFIFE-HBBIEUQ‡

B.8.4.3. In de parlementaire voorbereiding verantwoordt de wetgever die manier van werken door te verwijzen naar de technische aard van de identificatiegegevens en identificatiedocumenten, de noodzaak om de oplijsting daarvan te kunnen aanpassen in het licht van gewijzigde inzichten, en het feit dat ook in het kader van de dataretentie die gegevens niet in het bij het arrest van het Hof nr. 57/2021 van 22 april 2021 vernietigde artikel 126 van de wet van 13 juni 2005 zelf werden opgesomd.

Nog afgezien van het feit dat die argumenten de afwezigheid van een uitdrukkelijke en ondubbelzinnige machtiging niet kunnen verklaren, volstaan de technische aard van identificatiegegevens en identificatiedocumenten en de aanpasbaarheid van een dergelijke oplijsting niet om te besluiten dat een verankering ervan in een wetskrachtige norm de wetgever niet in staat zou stellen een doelstelling van algemeen belang te verwezenlijken. Ook een wetskrachtige norm kan immers worden gewijzigd. De Ministerraad toont niet aan dat een wijziging van die identificatiegegevens zo dringend kan zijn dat het normale verloop van de wetgevende procedure niet kan worden gevolgd. Een oplijsting van identificatiegegevens en identificatiedocumenten is ook niet dermate complex dat zij niet in een wetskrachtige norm kan worden opgenomen. Tot slot kan de wetgever een schending van de Grondwet niet rechtvaardigen door te verwijzen naar een andere wetsbepaling die mogelijk dezelfde ongrondwettigheid bevatte.

B.8.4.4. Artikel 127 van de wet van 13 juni 2005 bakent de uitvoeringsbevoegdheid van de Koning om te bepalen welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen, overigens onvoldoende af. Wat de identificatiedocumenten betreft, vermeldt het slechts dat het moet gaan om documenten waarop het rijksregisternummer voorkomt. Wat de andere identificatiegegevens dan het rijksregisternummer betreft, bevat het geen enkele precisering.

(...)

B.9.1. Uit het voorgaande blijkt dat artikel 127 van de wet van 13 juni 2005, zoals gewijzigd bij artikel 2 van de bestreden wet, het wettigheidsbeginsel gewaarborgd door artikel 22 van de Grondwet schendt, zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen. In die mate dient artikel 2 van de bestreden wet te worden vernietigd.

(...)

B.9.3. Aangezien de vastgestelde schending slechts betrekking heeft op artikel 22 van de Grondwet, en niet op de in het middel aangevoerde normen van Europees Unierecht, staat het aan het Hof om, op grond van artikel 8, derde lid, van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof, die gevolgen van de vernietigde bepalingen aan te wijzen welke als gehandhaafd moeten worden beschouwd of voorlopig gehandhaafd worden voor de termijn die het vaststelt.

De vastgestelde schending van artikel 22 van de Grondwet heeft geen betrekking op de aard en inhoud van de identificatiegegevens of identificatiedocumenten zoals die thans zijn geregeld in het koninklijk besluit van 27 november 2016 en die buiten de toetsingsbevoegdheid van het Hof vallen. Zij heeft slechts betrekking op het feit dat die gegevens en documenten in een wetskrachtige bepaling dienden te worden opgesomd.

Aan de wetgever moet bijgevolg de nodige tijd worden gegeven om in die wettelijke grondslag te voorzien, zonder dat in tussentijd de door de bestreden bepaling geregelde identificatie van de eindgebruikers van vooraf betaalde belkaarten dient te worden vernietigd. Die termijn dient bovendien voldoende lang te zijn om de wetgever toe te laten die wettelijke grondslag af te stemmen op de nieuwe dataretentieregeling die ingevolge het arrest van het Hof nr. 57/2021 van 22 april 2021 in voorbereiding is.

‡LW-AGFWNFIFE-HBBIEUQ‡

Bijgevolg dienen de gevolgen van de bestreden bepaling te worden gehandhaafd zoals aangegeven in het dictum.

Ten aanzien van het tweede middel

(...)

B.15.2. De thans bestreden wet heeft daarentegen slechts betrekking op de in artikel 127 van de wet van 13 juni 2005 bedoelde gegevens aan de hand waarvan de eindgebruiker van een elektronische-communicatiedienst die wordt geleverd op basis van een vooraf betaalde belkaart kan worden geïdentificeerd. Artikel 12, tweede lid, van het koninklijk besluit van 27 november 2016 bepaalt dat die identificatiegegevens kunnen verschillen afhankelijk van de gekozen identificatiemethode, maar somt tevens op limitatieve wijze de identificatiegegevens op die de betrokken onderneming maximaal mag bewaren:

"1° de naam en voornaam;

2° het geslacht;

3° de nationaliteit;

4° de geboorteplaats en -datum;

5° het adres van de woonplaats, het e-mailadres en het telefoonnummer;

6° het rijksregisternummer;

7° het nummer van het identiteitsstuk, het land van uitgifte van het document wanneer het een buitenlands document betreft en de geldigheidsdatum van het document;

8° de referenties van de betalingstransactie, conform artikel 17;

9° het verband van de voorafbetaalde kaart met het product waarvoor de eindgebruiker reeds geïdentificeerd is, conform artikel 18;

10° de foto van de eindgebruiker, maar enkel voor andere documenten dan de Belgische elektronische identiteitskaart".

Gelet op de gedeeltelijke vernietiging bedoeld in B.9.1 en de handhaving van de gevolgen bedoeld in B.9.3 dient de wetgever vóór de datum vermeld in het dictum de identificatiegegevens en identificatiedocumenten die voor de toepassing van artikel 127 van de wet van 13 juni 2005 kunnen dienen, in een wetsbepaling op te nemen.

B.15.3. Die persoonsgegevens zijn geen verkeers- en locatiegegevens, maar slechts de gegevens die gewoonlijk worden gehanteerd om iemand te identificeren. Het is niet mogelijk om aan de hand van die gegevens alleen iemands verplaatsingen, communicaties, activiteiten of sociale relaties te volgen, noch om een persoonlijk profiel op te stellen dat toelaat precieze conclusies te trekken over iemands seksuele geaardheid, overtuigingen en gezondheid. Zij geven op zich dus geen gevoelige informatie over het privéleven prijs.

Het is juist dat die identificatiegegevens vervolgens kunnen worden gekoppeld aan andere gegevens en op die manier kunnen bijdragen aan het vrijgeven van dergelijke gevoelige informatie over iemands privéleven. Die andere gegevens dienen dan evenwel op een andere manier te worden verzameld, en ook die verzameling dient te geschieden met eerbied voor de toepasselijke wetgeving en voor de grondrechten van de betrokkene.

Bijgevolg dient de bestaanbaarheid van de bestreden wet met het recht op eerbiediging van het privéleven te worden beoordeeld aan de hand van de in B.14.3 vermelde criteria.

‡LW-AGFWNFIFE-HBBIEUQ‡

B.16.1. De materiële en procedurele voorwaarden voor de verzameling, verwerking en bewaring van de identificatiegegevens van eindgebruikers van een elektronische-communicatienetwerk op basis van een vooraf betaalde belkaart worden geregeld in de artikelen 126 en 127 van de wet van 13 juni 2005 en in de koninklijke besluiten van 19 september 2013 en 27 november 2016.

(...)

B.16.8.5. Die bepalingen regelen op duidelijke en nauwkeurige wijze de materiële en procedurele voorwaarden waaronder die autoriteiten toegang kunnen hebben tot de krachtens artikel 127 van de wet van 13 juni 2005 verwerkte identificatiegegevens.

Wanneer zij zich toegang tot die gegevens verschaffen, dienen die autoriteiten niet alleen de in B.16.8.2 tot B.16.8.4 vermelde regels na te leven, maar ook de grondrechten van de eindgebruiker te eerbiedigen, zoals die onder meer zijn gewaarborgd door de [verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna "AVG")], de artikelen 6 en 8 van het Europees Verdrag voor de rechten van de mens en de artikelen 7, 8 en 47 van het Handvest.

B.16.8.6. In dat verband verwijzen de verzoekende partijen naar het arrest van de grote kamer van het Hof van Justitie van 2 maart 2021 in zake *Prokuratuur* (C-746/18, punten 50 tot 56), waarin het Hof van Justitie volgens hen eist dat een onafhankelijke bestuurlijke autoriteit of een rechter elk verzoek tot toegang voorafgaandelijk toetst aan de toepasselijke nationale regels en grondrechten en waarin het volgens hen preciseert dat het openbaar ministerie, dat de onderzoeksprocedure leidt en in voorkomend geval optreedt als aanklager, niet over de vereiste onafhankelijkheid beschikt om die toetsing te kunnen doorvoeren.

Dat arrest had evenwel betrekking op een verzoek van het openbaar ministerie om toegang te krijgen tot verkeers- en locatiegegevens. Zoals uiteengezet in B.14.3, vereisen het Hof van Justitie en het Europees Hof voor de Rechten van de Mens daarentegen geen voorafgaande rechterlijke of bestuurlijke toetsing van een verzoek om toegang tot identificatiegegevens. Bijgevolg verzet het recht op eerbiediging van het privéleven zich niet tegen een verzoek tot toegang tot dergelijke gegevens dat uitgaat van het openbaar ministerie.

B.16.8.7. Wel dient het verzoek om toegang tot de krachtens artikel 127 van de wet van 13 juni 2005 verwerkte identificatiegegevens steeds *in concreto* te worden gemotiveerd door het verband aan te tonen tussen die gegevens en de objectieve elementen die de initiële concrete verdenking van de betrokken eindgebruiker voor een specifiek misdrijf ondersteunen. Tevens dient te worden gemotiveerd dat er niet meer gegevens worden opgevraagd dan strikt noodzakelijk is in het licht van het lopende onderzoek. Een dergelijke motivering mag geen gebruik maken van standaardformuleringen of stijlformules.

(...)

B.22. Artikel 127 van de wet van 13 juni 2005 heeft slechts betrekking op de bewaring en verwerking van de identificatiegegevens bedoeld in artikel 12 van het koninklijk besluit van 27 november 2016. Dergelijke gegevens geven op zich geen inzicht in de persoonlijke standpunten van de geïdentificeerde persoon. Ook de verkeers- en locatiegegevens waaraan zij zouden kunnen worden gekoppeld, maken op zich geen meningsuiting uit.

‡LW-AGFWNFIFE-HBBIEUQ‡

Pas wanneer die gegevens tevens zouden worden gekoppeld aan de inhoud van een gevoerde communicatie, en de analyse daarvan aanleiding geeft tot verdere maatregelen, zoals het voeren van een onderzoek door de inlichtingen- en veiligheidsdiensten of het opstarten van een strafrechtelijk onderzoek, kan dat resulteren in een beperking van de vrijheid van meningsuiting, de vrijheid om informatie te verwerven, de persvrijheid of het bronnengeheim.

Zoals uiteengezet in B.15.3 dient een koppeling van identificatiegegevens aan andere metadata of aan de inhoud van een communicatie evenwel te zijn gebaseerd op een duidelijke en ondubbelzinnige wetsbepaling, dient zij de materiële en procedurele voorwaarden daarvan na te leven en dient zij in overeenstemming met de grondrechten van de betrokkene te gebeuren.

Een dergelijk onrechtstreeks verband tussen de bestreden afschaffing van de anonimiteit van vooraf betaalde belkaarten en de inhoud van gevoerde communicaties volstaat niet om de bestreden wet als een beperking op de vrijheid van meningsuiting aan te merken. De loutere verzameling van identificatiegegevens van alle eindgebruikers van een elektronische-communicatienetwerk kan in een democratische rechtsstaat niet de vrees rechtvaardigen dat alle communicatie over dat netwerk door de overheid zal worden gemonitord. De bestreden wet kan er bijgevolg op zich niet toe leiden dat personen worden ontmoedigd om hun mening te uiten of om informatie te delen met journalisten of politici.

(...)

Ten aanzien van het derde middel

(...)

B.24.3. De bestreden bepaling stelt geen gedragingen strafbaar en bepaalt geen straffen voor specifieke misdrijven. In tegenstelling tot wat de verzoekende partijen aanvoeren, bevat zij evenmin een automatische toerekenbaarheid aan de geïdentificeerde eindgebruiker van een vooraf betaalde belkaart van de misdrijven die worden ontdekt of bewezen na analyse van het gebruik van die belkaart. Artikel 127, § 1, derde lid, van de wet van 13 juni 2005 bevat slechts het weerlegbare vermoeden dat die eindgebruiker ook degene is die deze belkaart gebruikt. Het strafrechtelijk wettigheidsbeginsel is niet van toepassing op een dergelijke bepaling.

B.26.2. De bestreden bepaling vestigt bijgevolg geen automatische strafrechtelijke verantwoordelijkheid of objectieve aansprakelijkheid van de geïdentificeerde eindgebruiker van een vooraf betaalde belkaart voor het gebruik dat een derde daarvan maakt. Zij heeft voornamelijk een waarschuwingsfunctie, aangezien zij het uitgangspunt van elk strafrechtelijk onderzoek en van elk onderzoek door de inlichtingen- en veiligheidsdiensten in herinnering brengt, namelijk het uitgangspunt dat de eigenaar of gewoonlijke gebruiker van een voorwerp vermoedelijk degene is die het heeft gebruikt om een misdrijf te plegen of om de nationale veiligheid te bedreigen. De onderzoekers verlaten dat uitgangspunt zodra het wordt ontkracht door de verzamelde bewijselementen.

B.26.3. De bestreden bepaling houdt aldus verband met de doelstellingen die de wetgever met artikel 127 van de wet van 13 juni 2005 nastreeft, met name in noodsituaties en onderzoeken waarmee tijdsdruk gepaard gaat.

B.26.4. De bestreden bepaling speelt bovendien vaak in het kader van misdrijven of bedreigingen van de nationale veiligheid die ernstige gevolgen kunnen hebben voor de fysieke integriteit van personen of aanzienlijke maatschappelijke onrust kunnen veroorzaken.

‡LW-AGFWNFIFE-HBBIEUQ‡

B.26.5. De geïdentificeerde eindgebruiker beschikt over verschillende mogelijkheden om zich te verdedigen tegen strafrechtelijke vervolgingen die zouden kunnen voortvloeien uit het gebruik dat een derde van zijn vooraf betaalde kaart heeft gemaakt. Indien hij aan de onderzoekers meldt wie gebruik heeft gemaakt van zijn vooraf betaalde belkaart, dienen zij diens betrokkenheid te onderzoeken.

De bestreden bepaling stelt overigens slechts een weerlegbaar vermoeden in, dat door de beklaagde met alle middelen van recht kan worden weerlegd. Zij verbiedt hem niet om alle feitelijke elementen aan te dragen die zijn betrokkenheid bij de gepleegde misdrijven of bij de onderzochte bedreigingen voor de nationale veiligheid ontkrachten.

Daarnaast doet de bestreden bepaling geen afbreuk aan het beginsel dat het in een strafproces aan het openbaar ministerie toekomt de schuld van de beklaagde te bewijzen. Het staat aan de strafrechter de bewijswaarde van alle bewijselementen, met inbegrip van de uitleg van de beklaagde, te onderzoeken en daarbij diens recht op een eerlijk proces te eerbiedigen.

Aangezien de bestreden bepaling aldus geen afbreuk doet aan het recht van verdediging van de beklaagde, brengt zij evenmin het vermoeden van onschuld in het gedrang.

B.26.6. In tegenstelling tot hetgeen de verzoekende partijen aanvoeren, geldt het voorgaande evenzeer voor de betrokkenheid van de geïdentificeerde eindgebruiker bij de terroristische misdrijven vermeld in de artikelen 137 tot 141*ter* van het Strafwetboek. Hij kan slechts als mededader of medeplichtige van dergelijke misdrijven worden veroordeeld indien het openbaar ministerie alle constitutieve elementen van die misdrijven, met inbegrip van het intentionele element, te zijnen aanzien bewijst. Het te goeder trouw ter beschikking stellen van een vooraf betaalde belkaart door een eindgebruiker die niet kon vermoeden dat zij zou worden gebruikt om een dergelijk misdrijf te plegen of voor te bereiden, kan op zich geen strafrechtelijke veroordeling verantwoorden.

(...)

Ten aanzien van het vierde middel

(...)

B.29.1. De toegang van een overheid tot bankgegevens valt onder het toepassingsgebied van het recht op eerbiediging van het privéleven, ongeacht of die gegevens privacygevoelig zijn en ongeacht of zij verband houden met de beroepsuitoefening (EHRM, 7 juli 2005, *M.N. e.a. t. San Marino*, §§ 51-55; 1 december 2015, *Brito Ferrinho Bexiga Villa-Nova t. Portugal*, § 44; 27 april 2017, *Sommer t. Duitsland*, § 48).

B.29.2. De toegang van de overheid tot bankgegevens dient gebaseerd te zijn op een specifieke wettelijke machtiging die het voorwerp ervan, alsook de drempel om er zich toegang toe te verschaffen, duidelijk en ondubbelzinnig afbakent. Dat voorwerp dient beperkt te zijn tot hetgeen noodzakelijk is in het licht van de nagestreefde wettige doelstelling, aangezien een te ruime toegang tot bankgegevens de overheid zou toelaten zich een gedetailleerd beeld te vormen van het privéleven van de betrokkene. De overheid mag slechts toegang tot dergelijke gegevens hebben indien zij over concrete aanwijzingen beschikt dat de houder van de bankrekening betrokken is bij een misdrijf. Tevens dient de wet te voorzien in maatregelen tegen misbruik, waaronder de waarborg dat de gegevens niet langer worden bewaard dan noodzakelijk in het licht van het gevoerde onderzoek. Tot slot dient een daadwerkelijk rechterlijk toezicht te bestaan op de naleving van die materiële en procedurele voorwaarden (EHRM, 27 april 2017, *Sommer t. Duitsland*, §§ 57-63).

‡LW-AGFWNFIFE-HBBIEUQ‡

B.30.1. De bestreden bepaling preciseert welke diensten over de in B.28.2 bedoelde machtiging beschikken en welke instellingen tot medewerking gehouden zijn.

Zij bakent ook op tweevoudige wijze de doelstelling van de bestreden maatregel af. Ten eerste beoogt hij hetzij de in artikel 127 van de wet van 13 juni 2005 bedoelde eindgebruiker van een vooraf betaalde belkaart te identificeren, hetzij de vooraf betaalde belkaart te identificeren die door een bepaald persoon wordt gebruikt. Ten tweede moet die identificatie passen in het kader van de opdrachten van de inlichtingen- en veiligheidsdiensten.

B.30.2. Het voorwerp van de onderzoeksdaad is beperkt tot één specifieke banktransactie, namelijk degene waarmee een vooraf betaalde belkaart is aangekocht. Een dergelijke onderzoeksdaad laat de inlichtingen- en veiligheidsdiensten slechts toe identificatiegegevens te verwerven, maar verschaft hen op zich geen verkeers- of locatiegegevens, noch toegang tot de gevoerde communicaties.

De bestreden bepaling laat hun evenmin toe alleen met die onderzoeksdaad andere financiële informatie met betrekking tot de houder van de bankrekening te verkrijgen. Aldus maakt zij het hun niet mogelijk zich louter aan de hand van de verworven identificatiegegevens een beeld te vormen van het bestedingsgedrag of enig ander privacygevoelig element met betrekking tot de houder van de bankrekening.

Zoals uiteengezet in B.15.3 kunnen die identificatiegegevens vervolgens weliswaar worden gekoppeld aan andere gegevens en kan de bestreden bepaling aldus bijdragen aan het vrijgeven van dergelijke gevoelige informatie, maar die informatie dient dan te worden verzameld aan de hand van andere onderzoeksdaden, die op hun beurt de toepasselijke wetgeving en de grondrechten van de betrokkene moeten eerbiedigen.

B.30.3. Zoals uiteengezet in B.3.3, kan de identificatie op grond van de bestreden bepaling noodzakelijk zijn naar gelang van de identificatiemethode waarvoor de eindgebruiker bij de aankoop van de vooraf betaalde belkaart heeft gekozen.

Indien hij bij de aankoop van de vooraf betaalde belkaart kiest voor de identificatie op grond van de onlinebetalingstransactie, kunnen de inlichtingen- en veiligheidsdiensten hem slechts identificeren indien zij over de referentie van de elektronische banktransactie beschikken en deze kunnen koppelen aan zowel de belkaart als de identiteit van de eindgebruiker (*Parl.St.*, Kamer, 2015-2016, DOC 54-1964/001, pp. 14-16).

(...)

B.30.4. Aangezien de bestreden bepaling de inlichtingen- en veiligheidsdiensten slechts machtigt om de bestreden onderzoeksdaad te stellen in het belang van de uitoefening van hun opdrachten, dienen zij daarbij steeds te beschikken over concrete aanwijzingen dat de identificatie van de eindgebruiker van een vooraf betaalde belkaart noodzakelijk is in het kader van de opdrachten die limitatief worden opgesomd in artikel 7 (Veiligheid van de Staat) en artikel 11 (Algemene Dienst Inlichting en Veiligheid) van de wet van 30 november 1998. Aangezien die opdrachten alle betrekking hebben op vitale belangen van de Natie, is bij het nemen van die maatregel steeds minstens een dreiging aanwezig dat zich een gebeurtenis met zeer ingrijpende maatschappelijke gevolgen zou voordoen.

(...)

‡LW-AGFWNFIFE-HBBIEUQ‡

Om die redenen,

het Hof,

– vernietigt artikel 2 van de wet van 1 september 2016 'tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst[en]', zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen;

– handhaaft de gevolgen van de vernietigde bepaling tot de inwerkingtreding van een wetskrachtige norm waarin die identificatiegegevens en identificatiedocumenten worden opgesomd en uiterlijk tot en met 31 december 2022;

– verwerpt het beroep voor het overige, onder voorbehoud van de in B.8.7.3, B.16.6, B.16.8.5, B.16.8.7, B.26.2, B.26.6 en B.30.4 vermelde interpretaties."

II. Strekking van de amendementen

De steller van de amendementen vat de strekking van de amendementen als volgt samen:

"1. Inleiding en/of retroacta

In zijn arrest nr. 57/2021 van 22 april 2021 heeft ons Grondwettelijk Hof de artikelen 2, b), 3 tot 11 en 14 van de wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie nietig verklaard. Deze wet staat bekend als de 'wet inzake gegevensbewaring'.

Deze wet voorzag in de verplichting voor aanbieders aan het publiek van telefoniediensten, via internet inbegrepen, van internettoegangsdiensten en van e-maildiensten via internet (ongeacht of zij bij het BIPT aangemelde operatoren waren of niet) om bepaalde, identificatie-, verkeers- en locatiegegevens te bewaren gedurende 12 maanden, opdat die gegevens beschikbaar zouden zijn voor strafrechtelijke doeleinden (strafrechtelijke onderzoeken) of voor het vervullen van de taken van de inlichtingen- en veiligheidsdiensten. Deze gegevens hebben geen betrekking op de inhoud van de communicatie.

De regering heeft een ontwerp van herstel van de 'wet inzake gegevensbewaring' voltooid. Dat ontwerp is goedgekeurd door de Ministerraad van 17/12/2021 (tweede lezing). Voor dat ontwerp werden alle noodzakelijke adviezen ontvangen en de regering was dus van plan om naar het Parlement te gaan zodra mogelijk.

‡LW-AGFWNFIFE-HBBIEUQ‡

Ons Grondwettelijk Hof heeft intussen op 18/11/2021 echter een nieuw arrest geveld met betrekking tot de wet van 1 september 2016, die werd aangenomen om een einde te maken aan de anonimiteit van de voorafbetaalde kaarten aan de hand waarvan mobiele diensten kunnen worden gebruikt (bellen, internettoegang, sms'en versturen, enz.) door de operatoren te verplichten om deze laatsten te identificeren. In dat arrest

– stelt het Hof het principe van identificatie van de abonnees van voorafbetaalde kaarten niet ter discussie;

– maar het vernietigt de wijziging aangebracht door de wet van 1 september 2016 in art. 127 van de telecomwet 'zij het slechts in zoverre het niet bepaalt welke identificatiegegevens worden verzameld en verwerkt en welke identificatiedocumenten in aanmerking komen'; volgens het Hof eist artikel 22 van het Hof dat deze gegevens en documenten worden opgesomd in de wet;

– behoudt het Hof de gevolgen van de vernietigde bepaling tot de inwerkingtreding van een wetskrachtige norm waarin die identificatiegegevens en identificatiedocumenten worden opgesomd en uiterlijk tot en met 31 december 2022.

Uit de analyse blijkt dat de artikelen 126 en 126/1 van de telecomwet, zoals beoogd in het ontwerp van herstel, inderdaad moeten worden herzien. Het zou immers paradoxaal en moeilijk te rechtvaardigen zijn:

– dat de identificatiegegevens die de operatoren moeten bewaren krachtens artikel 126 van de telecomwet worden vastgelegd bij koninklijk besluit, terwijl de identificatiegegevens die ze moeten bewaren krachtens artikel 127 van de wet volgens het Grondwettelijk Hof moeten worden opgelijst in de wet;

– in de wet de in artikel 127 bedoelde identificatiegegevens worden opgenomen maar dat de metagegevens (bijv. wie belt wie, wanneer en wat zijn de locatiegegevens), die zullen moeten bewaard worden krachtens artikel 126/1 van de telecomwet en waarvan moet worden beschouwd dat ze meer impact hebben op de persoonlijke levenssfeer van de betrokkenen (aangezien ze meer informatie over hun levensgewoonten onthullen) dan eenvoudige identificatiegegevens, mogen worden opgelijst in een koninklijk besluit.

Daaruit volgt dat die artikelen 126 tot 127 in het ontwerp van herstel moeten worden gewijzigd.

2. Toelichting bij het dossier

2.1. Wijzigingen in de telecomwet wat betreft de artikelen 126 en 126/1

Er wordt verwezen naar punt 1 hierboven. De gegevens die de operatoren moeten bewaren en die nu worden opgesomd in het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de telecomwet, zijn overgedragen naar de artikelen 126 en 126/2 van de telecomwet. De krachtens artikel 126/1 te bewaren gegevens werden opgenomen in een nieuw artikel 126/2 aangezien artikel 126/1 bijzonder lang is.

De geplande wijzigingen in het koninklijk besluit van 19 september 2013, dat ontdaan is van een groot deel van zijn kern, moeten dan ook worden aangepast.

2.2. Wijzigingen aan artikel 127 van de telecomwet en de verwante artikelen

Als reactie op het arrest van het Grondwettelijk Hof van 18/11/2021 wordt artikel 127 van de telecomwet gewijzigd zodat dat artikel voortaan de beoogde identificatiegegevens en -documenten opsomt.

‡LW-AGFWNFIFE-HBBIEUQ‡

2.3. Wijzigingen van bepaalde organieke wetten

Het huidige artikel 127 van de telecomwet werd ten uitvoer gebracht door het koninklijk besluit van 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische-communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart (hierna het koninklijk besluit 'voorafbetaalde kaarten'). Dit koninklijk besluit voorziet in verscheidene methodes voor directe identificatie van de abonnee (de operator wint rechtstreeks bij de operator de burgerlijke identiteit van de abonnee in) en een methode van indirecte identificatie van de abonnee. In geval van een online betaling van een voorafbetaalde kaart bewaart de operator bijvoorbeeld het betalingskenmerk, dat de overheid zal verstrekken aan een bank, en vraagt daarbij om hem de identiteit van de abonnee te verstrekken.

De nieuwe versie van artikel 127 geeft voortaan een opsomming van de methodes van indirecte identificatie die zijn toegestaan aangezien het gaat om een essentiële kwestie in de wetgeving.

Een aantal van deze methodes van indirecte identificatie vereisen de interventie van een derde die geen operator is teneinde de identificatie mogelijk te maken. Het gaat in het bijzonder over:

– de banksector (betalingskenmerk in het bezit van een operator en meegedeeld aan een bank om de identiteit van de abonnee te verkrijgen);

– de gesloten centra (die voorafbetaalde kaarten nemen voor de personen in deze centra en dus op hun niveau het verband leggen tussen een voorafbetaalde kaart en een identiteit);

– de rechtspersonen die de rol van tussenpersoon kunnen spelen in de verdeling van de voorafbetaalde kaarten of intekeningen op abonnementen, met name om personen in een kwetsbare situatie te helpen (bijv. verblijfplaatsen voor oudere personen).

In voorkomend geval dienen de organieke wetten te worden gewijzigd om zich ervan te vergewissen dat de autoriteiten van deze derden de identiteit van de abonnee kunnen krijgen op basis van de informatie waarover zij reeds beschikken via de indirecte methode.

Voordien konden zowel de inlichtingen- en veiligheidsdiensten als de procureur des Konings zich richten tot de banken om de identiteit van de abonnee van de operator op te vragen wanneer de operator toestemming had gegeven om zijn abonnees te identificeren via een kenmerk van de betaling via de bank. Dat werd bekrachtigd in het Wetboek van Strafvordering en werd uitgebreid met de officieren van gerechtelijke politie van met de officieren van gerechtelijke politie van het BIPT, de FSMA en het directoraatgeneraal Gezondheid en consumentenbescherming."

VOORAFGAANDE VORMVEREISTEN

In de adviesaanvraag staat het volgende:

"Une consultation publique de 4 semaines, conformément à l'article 18 du Code européen des communications électroniques, a en outre démarré le 25 février 2022 via le site Internet de l'IBPT et l'avis des trois autorités compétentes en matière de protection des données a également été demandé.

‡LW-AGFWNFIFE-HBBIEUQ‡

À cet égard, nous pouvons d'ores-et-déjà vous communiquer que, vu que ces modifications sous forme d'amendements concernent essentiellement les traitements effectués par les opérateurs (collecte de données d'identification/de localisation), le C.O.C. et le Comité R considèrent qu'ils ne sont pas compétents pour rendre un avis.

L'APD nous a indiqué qu'elle rendrait son avis dans un délai d'un mois (la demande d'avis datant du 25 février 2022).

Enfin, le Comité interministériel des télécommunications, de la radiodiffusion et de la télévision sera consulté et l'accord du Comité de concertation sera également demandé."[6]

Uit het voorgaande volgt dat de om advies voorgelegde tekst ten gevolge van het vervullen van de voormelde verplichte vormvereisten nog andere wijzigingen kan ondergaan dan die welke uit het advies van de afdeling Wetgeving zouden kunnen voortvloeien.

Ook al is de afdeling Wetgeving ertoe gehouden om advies uit te brengen over een wetgevend voorontwerp en al zijn niet alle verplichte voorafgaande vormvereisten vervuld, mogen aan haar evenwel alleen *a priori* definitieve ontwerpen of voorontwerpen van tekst voorgelegd worden, niet alleen om een onnodig onderzoek te vermijden van een tekst die naderhand nog gewijzigd zal worden, maar ook om te vermijden dat een ontwerp wegens wijzigingen die niet het gevolg zijn van haar advies, opnieuw om advies aan haar voorgelegd zou moeten worden.

De steller van de amendementen wordt verzocht zich voortaan aan die regel te houden.[7]

ONDERZOEK VAN DE AMENDEMENTEN

Amendement nr. 1
Ontworpen artikel 126 van de wet van 13 juni 2005

1. Om tegemoet te komen aan de kritiek die het Grondwettelijk Hof in zijn arrest nr. 158/2021 van 18 november 2021 geuit heeft met betrekking tot de schending van het legaliteitsbeginsel vervat in artikel 22 van de Grondwet, strekt amendement nr. 1 ertoe voortaan in het ontworpen artikel 126, § 1, van de wet van 13 juni 2005 te bepalen welke gegevens bewaard moeten worden door de operatoren die aan de eindgebruikers elektronische-communicatiediensten bieden, alsook door de operatoren die de elektronische-communicatienetwerken aanbieden waarmee deze diensten verstrekt kunnen worden, voor zover ze die gegevens verwerken of genereren in het kader van de verstrekking van die netwerken of diensten.[8]

[6] Advies nr. 66/2022 d.d. 1 april 2022 van de Gegevensbeschermingsautoriteit is op 12 april 2022 aan de afdeling Wetgeving bezorgd.

[7] Zie, in die zin, advies 69.381/4, 91.

[8] De meeste van die gegevens zijn thans vervat in paragraaf 1 van de artikelen 3 tot 6 van het koninklijk besluit van 19 september 2013 'tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie'.

‡LW-AGFWNFIFE-HBBIEUQ‡

Bepaalde van die gegevens kunnen gekwalificeerd worden als gegevens betreffende de burgerlijke identiteit van de gebruikers in de zin van de rechtspraak van het Hof van Justitie of op zijn minst als gegevens die soortgelijke risico's inhouden voor het privéleven van de gebruikers.[9] De andere gegevens vormen gegevens betreffende het verkeer of locatiegegevens, zoals bijvoorbeeld de IP-adressen toegekend aan de bron van een verbinding.

De toegang tot die gegevens, die in het ontworpen artikel 127/1, § 3, van de wet van 13 juni 2005 geregeld wordt, lijkt *a priori* geen moeilijkheden op te leveren in het licht van het door het Hof van Justitie vastgestelde kader.

De indiener van het amendement dient zich er evenwel van te vergewissen dat de gegevens opgenomen in het ontworpen artikel 126, § 1, die geen betrekking hebben op de burgerlijke identiteit, op het gebied van het traceren van de gebruiker geen soortgelijke risico's inhouden als die welke door het Hof van Justitie geschetst zijn met betrekking tot de IP-adressen toegewezen aan de bron van de verbinding,[10] in welk geval de toegang tot die gegevens eveneens beperkt zou moeten worden, naar het voorbeeld van wat bepaald wordt in het ontworpen artikel 127/1, § 3, vierde lid.[11]

Het dispositief moet dienovereenkomstig herzien worden.

[9] In zijn arrest C-511/18 heeft het Hof het volgende geoordeeld: "157. Wat ten slotte de gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronische-communicatiemiddelen betreft, moet worden opgemerkt dat met die gegevens alleen noch de datum, het tijdstip, de duur en de ontvangers van de communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Die gegevens verschaffen dus, afgezien van de contactgegevens van de betrokken gebruikers, zoals hun adres, geen informatie over wat die personen hebben gecommuniceerd en dus over hun privéleven. De inmenging die de bewaring van die gegevens met zich brengt, kan derhalve niet als 'ernstig' worden aangemerkt (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punten 59 en 60).
158. Hieruit volgt dat, overeenkomstig hetgeen is uiteengezet in punt 140 van het onderhavige arrest, wettelijke maatregelen die betrekking hebben op de verwerking van die gegevens als zodanig, in het bijzonder op de bewaring van en de toegang tot die gegevens met als enige doel de betrokken gebruiker te identificeren, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van [de] richtlijn genoemde doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 62)."

[10] Zie arrest C-511/18 (overweging 153) en arrest C-746/18 (overweging 35) van het Hof van Justitie evenals, in het bijzonder wat de gegevens betreft waarmee de eindapparaten van de eindgebruikers technisch geïdentificeerd kunnen worden, advies 108/2021 (overweging 102) en advies 66/2022 (voetnoot 12) van de Gegevensbeschermingsautoriteit. Zie ook meer in het algemeen advies 69.381/4, 157 tot 159.

[11] Die bepaling luidt als volgt: "In afwijking van het tweede lid, is een verzoek van een autoriteit om van een operator een IP-adres te krijgen dat is toegewezen aan de bron van een verbinding, enkel toegestaan voor de doeleinden van de vrijwaring van de nationale veiligheid, de bestrijding van zware criminaliteit, de preventies van ernstige dreigingen voor de openbare veiligheid en de vrijwaring van de vitale belangen van een fysieke persoon, wanneer die autoriteit in staat zou zijn om, met behulp van de informatie in haar bezit en de aan de bron van de verbinding toegewezen IP-adressen die ze van de operator heeft verkregen, het traject van een eindgebruiker op internet te achterhalen."

‡LW-AGFWNFIFE-HBBIEUQ‡

2. In het eerste lid, 17°, en in het tweede lid van het ontworpen artikel 126, § 1, staat het volgende:

> "Onverminderd de AVG en de wet van 30 juli 2018, bewaren de operatoren die aan de eindgebruikers elektronische-communicatiediensten bieden, alsook de operatoren die de elektronische-communicatienetwerken aanbieden waarmee deze diensten verstrekt kunnen worden, de volgende gegevens voor zover ze die verwerken of genereren in het kader van de verstrekking van die netwerken of diensten:
>
> (…)
>
> 17° de andere identifier[s] met betrekking tot de eindgebruiker, tot de eindapparatuur of tot de apparatuur het dichtst bij die eindapparatuur die uit de technologische evolutie resulteren en die door de Koning bepaald worden, op voorwaarde dat dit besluit door de wet wordt bekrachtigd binnen twaalf maanden na de bekendmaking van dit besluit.
>
> Het koninklijk besluit bedoeld in het eerste lid, 17°, slaat niet op de inhoud van de elektronische communicatie, noch op de elektronische-communicatiemetagegevens die informatie geven over de geadresseerde van de communicatie, zoals het IP-adres van de geadresseerde van de communicatie, of over de locatie van de eindapparatuur."

Ter wille van de overeenstemming met arrest nr. 158/2021 van het Grondwettelijk Hof d.d. 18 november 2021[12] moet de indiener van het amendement in de verantwoording van het amendement aantonen in welk opzicht het "normale verloop van de wetgevende procedure" van dien aard is dat die identifiers niet op tijd bepaald kunnen worden. Bij die gelegenheid moet hij preciseren in welk opzicht een termijn van twaalf maanden in overeenstemming is met de lering van voornoemd arrest, waarin vereist wordt dat het besluit "binnen een relatief korte termijn" bekrachtigd wordt.

Het spreekt ten slotte van zelf dat, indien de betrokken besluiten niet binnen de voorgeschreven termijn bekrachtigd worden, ze geacht moeten worden nooit uitwerking te hebben gehad.[13]

Het ontworpen artikel 126, § 1, eerste lid, 17°, en in voorkomend geval de verantwoording ervan moeten in het licht van deze opmerking herzien worden.

Dezelfde opmerking geldt *mutatis mutandis* voor het ontworpen artikel 126/2, § 2, eerste lid, 12°, en voor het ontworpen artikel 127, § 5, eerste lid, 32°.

3. Artikel 126, § 1, derde lid, 2°, strekt ertoe aan de Koning machtiging te verlenen om "de vereisten [te bepalen] waaraan deze gegevens moeten beantwoorden".

[12] Zie de overwegingen B.8.4.1 tot B.8.4.4.

[13] Zie advies 68.936/AV van 7 april 2021 over een voorontwerp dat geleid heeft tot de wet van 14 augustus 2021 'betreffende de maatregelen van bestuurlijke politie tijdens een epidemische noodsituatie', *Parl.St.* Kamer 2020-21, nr. 55-1951/001, 55-127, http://www.raadvst-consetat.be/dbx/adviezen/68936.pdf, opmerking 102.

‡LW-AGFWNFIFE-HBBIEUQ‡

In de verantwoording van het amendement dient gepreciseerd te worden wat bedoeld wordt met het woord "vereisten" teneinde uitdrukkelijk en ondubbelzinnig het onderwerp van die machtiging vast te stellen overeenkomstig hetgeen in artikel 22 van de Grondwet vereist wordt.

Dezelfde opmerking geldt voor het ontworpen artikel 126/2, § 4.

4. In artikel 126, § 2, vijfde lid, moeten de woorden "tweede lid" vervangen worden door de woorden "derde lid".

Amendement nr. 3

Ontworpen artikel 126/2 van de wet van 13 juni 2005

1. Amendement n° 3 strekt ertoe in het ontworpen artikel 126/2, § 2, vast te stellen welke gegevens bewaard moeten worden door de operatoren die aan de eindgebruikers elektronische-communicatiediensten aanbieden, alsook door de operatoren die de onderliggende elektronische-communicatienetwerken aanbieden, voor de geografische zones bedoeld in het ontworpen artikel 126/1, § 3.[14]

In verband met het gegeven vermeld in het ontworpen artikel 126/2, § 2, eerste lid, 7°,[15] staat in de verantwoording van het amendement het volgende:

> "[Deze bepaling] preciseert de locatiegegevens die moeten worden bewaard in het kader van een communicatie (elke oproep of sms of ander type van binnenkomend of uitgaand bericht). In het kader van de internettoegangsdienst bestaat de communicatie in elk gegeven ontvangen door de eindgebruiker (bijv. alle ontvangen informatie zodra 4G is geactiveerd) of verzonden informatie (bijv. bezoek aan een website)."

Uit die uitleg kan niet opgemaakt worden welke elementen kunnen waarborgen dat de bewaring van dat gegeven verenigbaar is met het voorbehoud dat de Gegevensbeschermingsautoriteit gemaakt heeft in haar advies nr. 108/2021, naar luid waarvan "de bewaring van verkeersgegevens geen specifieke url van de door de betrokkenen bezochte webpagina's mag bevatten of mag toelaten die url's af te leiden".[16]

De verantwoording van het amendement moet dienovereenkomstig aangevuld worden.

---

[14] De meeste van die gegevens staan telkens vermeld in paragraaf 2 van de artikelen 3 tot 6 van het koninklijk besluit van 19 september 2013.

[15] Namelijk "de gegevens voor het identificeren en het lokaliseren van de cellen of andere netwerkaansluitpunten, die werden gebruikt voor de communicatie, van de start tot het einde van de communicatie alsook de exacte data en tijdstippen van deze verschillende locaties".

[16] Zie overweging 114 van advies nr. 108/2021. De steller van het amendement heeft aan die opmerkingen overigens gevolg gegeven wat de gegevens bedoeld in het ontworpen artikel 126/2, § 2, eerste lid, 3°, betreft ("voor de elektronische-communicatiediensten met uitzondering van de internettoegangsdiensten, het IP-adres dat gebruikt is door de geadresseerde van de communicatie, het tijdstempel alsook, in geval van gedeeld gebruik van een IP-adres van de geadresseerde, de poorten die aan hem zijn toegewezen") en wel om de volgende reden: "Dat gegeven wordt bewaard wat betreft andere elektronische-communicatiediensten dan de internettoegangsdiensten. In haar advies nr. 108/2021 van 28 juni 2021 benadrukt de Gegevensbeschermingsautoriteit immers dat de bewaring van de

‡LW-AGFWNFIFE-HBBIEUQ‡

2. Zoals door de Gegevensbeschermingsautoriteit opgemerkt wordt,[17] geeft de steller van het amendement geen afdoende verantwoording van de noodzakelijkheid en de strikte proportionaliteit van de verplichting om de gegevens bedoeld in het ontworpen artikel 126/2, § 2, eerste lid, 9° en 10°, te bewaren in het licht van de doeleinden inzake de vrijwaring van de nationale veiligheid, de strijd tegen zware criminaliteit en de preventie van ernstige dreigingen van de openbare veiligheid, vermeld in het ontworpen artikel 126/1, § 1, derde lid.[18]

De verantwoording van het amendement moet dienovereenkomstig aangevuld worden.

3. Bij het ontworpen artikel 126/2, § 2, eerste lid, 11°, wordt aan de operatoren de verplichting opgelegd om, "wanneer een van de voormelde gegevens niet beschikbaar is, elk gegeven met een gelijkwaardige functie [te bewaren]".

Zoals in de verantwoording van het amendement uitgelegd wordt, kunnen de technologische evolutie en de verscheidenheid aan technische kenmerken van de diensten waarvoor die verplichting tot bewaring geldt, het moeilijk maken om alle gegevens te bepalen die onder die verplichting vallen.

Gelet op de ernstige inmenging in het recht van de betrokken personen die voortvloeit uit een dergelijke verplichting tot het bewaren van gegevens – op de niet-naleving waarvan er bovendien strafrechtelijke straffen gesteld worden[19] – die aan de operatoren opgelegd wordt, dient evenwel in de wet, op exhaustieve en voorzienbare wijze, gepreciseerd te worden welke gegevens in dat kader verzameld mogen worden.

verkeersgegevens geen specifieke URL van de door de betrokken personen bezochte websites mogen bevatten, of het niet mogelijk mag maken om dergelijke URL's af te leiden. Om die reden, is de bewaring van het IP-adres van bestemming uitgesloten voor de internettoegangsdiensten."

[17] Zie overweging 35 van advies nr. 66/2022 van 1 april 2022 van de Gegevensbeschermingsautoriteit.

[18] Zie overweging 11 van richtlijn 2002/58/CE, die als volgt luidt: "Deze richtlijn is evenmin [als] Richtlijn 95/46/EG van toepassing op vraagstukken met betrekking tot de bescherming van fundamentele rechten en vrijheden in verband met niet onder het Gemeenschapsrecht vallende activiteiten. Zij verandert bijgevolg niets aan het bestaande evenwicht tussen het recht van personen op persoonlijke levenssfeer en de mogelijkheid voor de lidstaten om de in artikel 15, lid 1, van deze richtlijn bedoelde maatregelen te nemen, die nodig zijn voor de bescherming van de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economisch welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de wetshandhaving op strafrechtelijk gebied. Bijgevolg doet deze richtlijn geen afbreuk aan de mogelijkheid voor de lidstaten om wettelijk toegestane interceptie van elektronische communicatie uit te voeren of andere maatregelen vast te stellen, wanneer dat voor één van voornoemde doeleinden noodzakelijk is, mits zij daarbij het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zoals geïnterpreteerd in de uitspraken van het Europees Hof voor de rechten van de mens, in acht nemen. Zulke maatregelen dienen passend te zijn voor, en strikt evenredig met, het beoogde doel en noodzakelijk in een democratische samenleving en moeten adequate waarborgen bevatten overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden."

[19] Zie het ontworpen artikel 145, § 1, (amendement nr. 8).

‡LW-AGFWNFIFE-HBBIEUQ‡

Een oplossing om aan al die vereisten te voldoen, zou erin kunnen bestaan de Koning ertoe te machtigen te bepalen op welke categorieën van gegevens het ontworpen artikel 126/2, § 2, eerste lid, 11°, betrekking zou kunnen hebben, voor zover ze "een gelijkwaardige functie" hebben in het licht van de technologische evolutie en van de technische verschillen tussen de diverse beoogde diensten, voor zover vaststaat dat de naleving van de parlementaire procedure het voor de wetgever onmogelijk maakt die gegevens vast te stellen en op voorwaarde dat het koninklijk besluit binnen een relatief korte termijn bij wet bekrachtigd wordt.

Het ontworpen artikel 126/2, § 2, eerste lid, 11°, moet in het licht van deze opmerking herzien worden.

4. In het ontworpen artikel 126/2, § 2, tweede lid, dient verwezen te worden naar het koninklijk besluit "bedoeld in het eerste lid, 12°".[20]

Amendement nr. 6

Ontworpen artikel 127 van de wet van 13 juni 2005

1. De vermelding van een "§ 2" ontbreekt in het dispositief van het amendement.

2. Uit de inleidende zin van het ontworpen artikel 127, § 1, zesde lid, vloeit voort dat alle indirecte identificatiemethodes aangewend kunnen worden voor de diensten opgesomd in dat lid, 1° tot 3°.

Het is de afdeling Wetgeving dan ook niet duidelijk hoe die inleidende zin verenigbaar zou zijn met de bepaling onder 2° van datzelfde lid, waarin sprake is van het specifieke geval waarin "de operator de indirecte identificatiemethode zoals bedoeld in paragraaf 9, eerste lid, 4° hanteert".

De redactie van het ontworpen artikel 127, § 1, zesde lid, 2°, moet herzien worden.

3. In het ontworpen artikel 127, § 1, zesde lid, 3°, moet de verwijzing naar het ontworpen artikel 127, § 5, "tweede lid" worden vervangen door een verwijzing naar het eerste lid van die bepaling.

4.1. Het ontworpen artikel 127, § 4, derde tot zevende lid, stelt het volgende:

> "Teneinde die betrouwbaarheid te garanderen en na machtiging van de minister en van de minister van Justitie, kan de operator of het verkooppunt van elektronische-communicatiediensten met de instemming van de abonnee en automatisch een vergelijking uitvoeren tussen de biometrische gegevens op de foto van het identiteitsdocument van de abonnee en deze van zijn gezicht.
>
> De machtiging wordt verleend aan een operator of aan een onderneming die de in het derde lid bedoelde vergelijkingsmethode aanbiedt.

[20] Als de steller van het amendement gevolg geeft aan de suggestie in opmerking 3, moet, in voorkomend geval, eveneens verwezen worden naar het koninklijk besluit bedoeld in het eerste lid, 11°.

‡LW-AGFWNFIFE-HBBIEUQ‡

De in het derde lid bedoelde machtiging heeft tot doel de betrouwbaarheid van deze vergelijking ten behoeve van de autoriteiten na te gaan.

De operator biedt de abonnee minstens een alternatieve manier aan om zich te identificeren.

De operator en het verkooppunt mogen deze biometrische parameters niet meedelen aan een derde als bedoeld in artikel 4, 10) van de AVG. Zij mogen deze maar verwerken binnen de limieten die nodig zijn om het in het derde lid beoogde doel van gezichtsvergelijking te verwezenlijken."

Deze bepaling maakt het voor de operator of het verkooppunt mogelijk de biometrische gegevens op de foto van het identiteitsdocument van de abonnee te vergelijken met die van zijn gezicht.

Deze bepaling geeft aanleiding tot de volgende opmerkingen.

4.2. Elke verwerking van persoonsgegevens moet onder meer voldoen aan de algemene vereisten van artikel 5, lid 1, van de AVG.

Een van die vereisten is het beginsel van de minimale gegevensverwerking, naar luidt waarvan de persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij verwerkt worden.

Met betrekking tot de betrokken identificatiemethode, die berust op de verwerking van biometrische gegevens, zijn de redenen die in de verantwoording van het amendement gegeven worden niet overtuigend.[21]

Het staat derhalve aan de indiener van het amendement om in de verantwoording ervan te preciseren op grond van welke elementen ervan uit kan worden gegaan dat het beginsel van de minimale gegevensverwerking *in casu* daadwerkelijk nageleefd is, terwijl er andere middelen bestaan die minder ingrijpend zijn in het licht van de persoonlijke levenssfeer en voldoende lijken om de identiteit van de abonnee aan te tonen, zelfs voor degenen die geen gebruik kunnen maken van de eID of van gekwalificeerde verleners van vertrouwensdiensten die een dienst voor gekwalificeerde elektronische handtekeningen aanbieden [22].

4.3. Overeenkomstig artikel 9, lid 1, van de AVG heeft de verwerking van biometrische gegevens met het oog op de unieke identificatie van een natuurlijk persoon betrekking op gevoelige gegevens en is ze in beginsel verboden.

Slechts wanneer aan een van de in artikel 9, lid 2, van de AVG gestelde voorwaarden voldaan is, kan een dergelijke verwerking aanvaard worden, mits de algemene vereisten van diezelfde verordening in acht genomen worden.

[21] Zie de overwegingen 51 tot 54 van advies nr. 66/2022 van de Gegevensbeschermingsautoriteit.

[22] Zoals zich, bijvoorbeeld, fysiek begeven naar het verkooppunt.

‡LW-AGFWNFIFE-HBBIEUQ‡

In casu is een dergelijke verwerking mogelijk krachtens artikel 9, lid 2, a), van de AVG indien

> "de betrokkene (…) uitdrukkelijke toestemming gegeven [heeft] voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven".

Om te voldoen aan de vereisten die uit die bepaling voortvloeien, dient artikel 127, § 4, derde tot achtste lid, aldus herzien te worden dat gepreciseerd wordt dat de uitdrukkelijke toestemming van de abonnee verkregen moet worden, met dien verstande dat de wilsuiting van de abonnee, overeenkomstig artikel 7 van de AVG, in samenhang gelezen met artikel 4. 11), vrij, specifiek, geïnformeerd en eenduidig moet zijn, hetgeen betekent dat de abonnee op de hoogte moet zijn van de doeleinden waarvoor die gegevens verzameld zullen worden en dat de voorgestelde alternatieve methode om zich te identificeren niet dermate dwingend mag zijn dat de abonnee geen andere keuze heeft dan de verwerking van zijn biometrische gegevens toe te staan.

Ten slotte moet in de ontworpen bepaling, zoals uit de verantwoording van het amendement blijkt, gepreciseerd worden dat de biometrische gegevens niet bewaard zullen worden zodra de vergelijking in kwestie gemaakt is.

Het ontworpen artikel 127, § 4, derde tot achtste lid, moet in het licht van deze opmerking herzien worden.

4.4. De betrokken ministers worden verzocht om, overeenkomstig het ontworpen artikel 127, § 4, derde lid, machtiging te verlenen voor de vergelijking van de biometrische gegevens van de abonnees met die van hun gezicht.

Bij de ontworpen bepaling wordt geen enkel criterium bepaald dat hun beoordelingsbevoegdheid voor het verlenen van de bewuste machtigingen op dat punt zou afbakenen.

Het in artikel 22 van de Grondwet neergelegde legaliteitsbeginsel en de rechtszekerheid vereisen dat de essentiële elementen van die criteria door de wetgever vastgesteld worden.

De ontworpen bepaling moet in die zin herzien worden.

5. Ter waarborging van de eerbiediging van de beginselen van integriteit en vertrouwelijkheid van de identificatiedocumenten, die uit artikel 5, van de AVG voortvloeien, zou in het ontworpen artikel 127, § 5, derde lid, bepaald moeten worden dat die documenten slechts gekopieerd mogen worden voor zover het niet mogelijk is om de identificatiegegevens op elektronisch en beveiligde wijze op te vragen en voor zover de operatoren technische maatregelen nemen om te voorkomen dat van het gekopieerde identiteitsdocument enige conforme reproductie gemaakt wordt.[23]

[23] Zie in die zin voetnoot 43 van advies 66/2022 van de Gegevensbeschermingsautoriteit.

‡LW-AGFWNFIFE-HBBIEUQ‡

Dezelfde opmerking geldt *mutatis mutandis* voor de soortgelijke verplichting die aan rechtspersonen opgelegd wordt in het ontworpen artikel 127, § 10, tweede lid, 4°.

6. Het ontworpen artikel 127, § 5, vierde en vijfde lid, luidt als volgt:

"Wanneer de abonnee een identificatiedocument zoals bedoeld in het eerste lid ter identificatie voorlegt en de operator niet in staat is om de betrouwbaarheid van de identiteit van de abonnee te garanderen aan de hand van dat document, kan hij aan de abonnee vragen om hem het volgende te verstrekken teneinde de betrouwbaarheid te vergroten:

– de facturen van leveranciers van verschillende producten of diensten, voor de elektronische-communicatiediensten die worden betaald nadat ze werden verstrekt;

– aanvullende informatie.

De operator houdt een kopie van deze facturen en informatie bij."

Die bepaling voldoet niet aan de vereisten qua voorzienbaarheid die gelden inzake het recht op privacy, doordat niet nauwkeurig genoeg bepaald wordt om welke facturen en aanvullende informatie het gaat, zodat het zou kunnen gaan om welke informatie ook betreffende een abonnee, hetgeen niet aanvaardbaar lijkt.

Op basis van de informatie waarover zij beschikt, ziet de afdeling Wetgeving bovendien niet in hoe een dergelijke maatregel pertinent of proportioneel zou kunnen zijn voor de behoeften qua identificatie van de abonnee.

Het ontworpen artikel 127, § 5, vierde en vijfde lid, moet in het licht van die opmerking herzien worden.

7. Het ontworpen artikel 127, § 5, zesde lid, luidt als volgt:

"De Koning kan een aantal specifieke, eventueel indirecte, identificatiemethodes toestaan voor personen die over geen enkel van de in het eerste lid bedoelde documenten beschikken."

Indien die machtiging inderdaad aldus begrepen moet worden dat de Koning daarbij gemachtigd wordt om identificatiegegevens en -documenten vast te stellen die niet in het ontworpen artikel 127 vermeld zijn,[24] schendt de aldus voorziene delegatie artikel 22 van de Grondwet, zoals geïnterpreteerd door het Grondwettelijk Hof, naar luid waarvan die essentiële elementen in een formele wet opgenomen moeten worden.[25]

[24] Dat blijkt inzonderheid uit artikel 127, § 6, dat als volgt luidt: "Onverminderd de gegevens die worden bewaard op basis van het koninklijk besluit dat eventueel is genomen ter uitvoering van paragraaf 5, [zesde] lid, […]."

[25] In het voorontwerp wordt die machtiging als volgt verantwoord: "Aan de Koning wordt de mogelijkheid gelaten om creatieve ad-hoc oplossingen te vinden voor personen die over geen enkele van de in artikel 127 vermelde identificatiedocumenten zouden beschikken."

‡LW-AGFWNFIFE-HBBIEUQ‡

Een dergelijke machtiging zou slechts aanvaardbaar zijn indien het koninklijk besluit in kwestie binnen een relatief korte termijn bij wet bekrachtigd zou worden en op voorwaarde dat de indiener van het amendement kan aantonen dat het door de inachtneming van de parlementaire procedure voor de wetgever onmogelijk zou zijn de identificatiegegevens en -documenten in kwestie tijdig te bepalen.

De voorliggende bepaling en, in voorkomend geval, de verantwoording ervan, moeten in het licht van deze opmerking herzien worden.

Dezelfde opmerking geldt *mutatis mutandis* voor de machtigingen vervat in de ontworpen artikelen artikel 127, § 6, tweede lid, tweede streepje en artikel 127, § 9, 5°.

8. In artikel 127, § 6, eerste lid, wordt de lijst bepaald van de identificatiegegevens die de operator "hooguit" dient te bewaren, en in het tweede lid van die paragraaf wordt de lijst vastgesteld van de identificatiegegevens die de operator "minimaal" moet bewaren.

Het is echter van tweeën één.

Ofwel zijn slechts de in het tweede lid vermelde gegevens noodzakelijk en voldoende voor de doeleinden qua identificatie van de gebruiker, aangezien het gaat om de gegevens die de operatoren "minimaal" moeten bewaren. In dat geval is er geen reden om te eisen dat ook de in het eerste lid vermelde gegevens bewaard zouden worden.

Ofwel zijn de in het eerste lid opgenomen gegevens eveneens noodzakelijk voor dat doeleinde, in die zin dat ze het mogelijk maken zich, met inachtneming van het beginsel van minimale gegevensverwerking, te vergewissen van de identiteit van de gebruiker, met dien verstande dat het voor de operatoren niet altijd mogelijk is die gegevens voor alle betrokken gebruikers te verzamelen. In dit laatste geval moet de redactie van het ontworpen artikel 127, § 6, herzien worden teneinde de wijze waarop de twee lijsten van gegevens zich tot elkaar verhouden, duidelijker tot uiting te laten komen, met name door in het eerste lid niet de gegevens te vermelden die reeds overeenkomstig het tweede lid bewaard moeten worden.

Het ontworpen artikel 127, § 6, en de verantwoording ervan moeten in het licht van deze opmerking herzien worden.

9. Het ontworpen artikel 127, § 6, eerste lid, 5°, luidt als volgt :

> "Onverminderd de gegevens die worden bewaard op basis van het koninklijk besluit dat eventueel is genomen ter uitvoering van paragraaf 5, [zesde] lid, bewaart de operator, wanneer hij de abonnee die een natuurlijke persoon is, identificeert via een directe identificatiemethode, hooguit de volgende identificatiegegevens:
>
> (…)
>
> 5° de foto van de abonnee, maar enkel voor andere identiteitsstukken dan de Belgische elektronische identiteitskaart."

‡LW-AGFWNFIFE-HBBIEUQ‡

De bewaring van een foto ter identificatie van een persoon – zoals bepaald bij het voorliggende dispositief – moet worden beschouwd als de verwerking van een biometrisch gegeven[26], hetgeen betekent dat aan een van de in artikel 9, lid 2, van de AVG genoemde gevallen moet worden voldaan om te kunnen overgaan tot een dergelijke verwerking.

Artikel 9, lid 2, g), van de AVG lijkt de basis te kunnen vormen waarop de foto in kwestie zou kunnen worden bewaard.

Die bepaling luidt als volgt :

> "[D]e verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene."

Het staat aan de steller van het amendement om te kunnen aantonen dat *in casu* aan de door deze bepaling gestelde eisen is voldaan.

De bepaling moet in het licht van die opmerking worden herzien. Zo nodig moet de motivering van het amendement dienovereenkomstig worden aangevuld.

10. In het ontworpen artikel 127, § 6, eerste lid, 8°, dient, althans in de motivering van het amendement, te worden verduidelijkt wat onder "het openbaar veiligheidsnummer" moet worden verstaan.

11. De steller van het amendement moet de verplichting om, overeenkomstig het ontworpen artikel 127, § 9, 3°, de geboorteplaats en -datum van de abonnee te verzamelen en te bewaren wanneer hij een onlinebetaling verricht, kunnen rechtvaardigen, aangezien de referentie van de verrichting alsook de naam en voornaam van de abonnee voldoende lijken te zijn om hem te kunnen identificeren[27].

[26] Zie, in die zin, overweging nr. 51 van de AVG : "De verwerking van foto's mag niet systematisch worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken. Dergelijke persoonsgegevens mogen niet worden verwerkt, tenzij de verwerking is toegestaan in in deze verordening vermelde specifieke gevallen, rekening houdend met het feit dat in de wetgeving van de lidstaten specifieke bepalingen inzake gegevensbescherming kunnen worden opgenomen teneinde de toepassing van de regels van deze verordening aan te passen met het oog op de vervulling van een wettelijke verplichting of met het oog op de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend".

[27] Zie in die zin overweging nr. 76 van advies 66/2022 van de Gegevensbeschermingsautoriteit.

‡LW-AGFWNFIFE-HBBIEUQ‡

12. Het ontworpen artikel 127, § 10, vijfde lid, luidt als volgt :

"De operator bewaart het chassisnummer van het voertuig waarin een van zijn simkaarten ("*subscriber identity/identification module"*) of een gelijkwaardige kaart werd ingebouwd, evenals de link tussen het chassisnummer en het nummer van deze kaart, vanaf de activeringsdatum van de elektronische-communicatiedienst tot twaalf maanden na de stopzetting van de dienst."

Het identificatienummer van een voertuig kan toegang verlenen tot heel wat gegevens over het desbetreffende voertuig en, onrechtstreeks, over zijn eigenaar[28].

Gelet op het doel van de identificatie van de eigenaar van het voertuig, dient te worden bepaald dat enkel die laatste informatie aan de autoriteiten zal kunnen worden verstrekt in het kader van hun opdrachten.

Het ontworpen artikel 127, § 10, vijfde lid, en de verantwoording ervan moeten worden herzien in het licht van die opmerking.

Amendement nr. 9

Artikel 40 van het wetsontwerp

In de verantwoording van artikel 40 die bij amendement nr. 9 in het wetsontwerp wordt opgenomen, wordt uitgelegd dat het ontworpen artikel 127 enkel van toepassing zal zijn "voor de contracten die na de inwerkingtreding van de wet worden gesloten".

Het verdient aanbeveling om die regeling van inwerkingtreding, die niet duidelijk uit het ontworpen dispositief blijkt, uitdrukkelijk over te nemen in artikel 40 van het wetsontwerp.

Bovendien moet de verantwoording van het amendement worden aangevuld, teneinde te verduidelijken wat wordt bedoeld met de woorden "contracten die na de inwerkingtreding van de wet worden gesloten". Dat gebrek aan precisie kan in de praktijk immers tot moeilijkheden leiden, aangezien het grote aantal aanvullende diensten die al dan niet kosteloos kunnen worden verleend aan personen die reeds een lopend contract met een operator hebben[29].

Artikel 40 van het wetsontwerp en de motivering ervan moeten worden herzien in het licht van die opmerking.

[28] Zie artikel 18 van de wet van 19 mei 2010 'houdende oprichting van de Kruispuntbank van de voertuigen' en artikel 2 van het koninklijk besluit van 8 juli 2013 'ter uitvoering van de wet van 19 mei 2010 houdende oprichting van de Kruispuntbank van de Voertuigen'.

[29] Zie in dat verband het ontworpen artikel 127, § 2, eerste lid, 1°, dat aldus de betalende elektronische-communicatiedienst omschrijft als de "elektronische-communicatiedienst waarbij de abonnee moet betalen aan de operator om de dienst te gebruiken of te blijven gebruiken, evenals elke elektronische-communicatiedienst die samen met deze dienst zonder meerkosten door de operator wordt aangeboden aan de abonnee".

‡LW-AGFWNFIFE-HBBIEUQ‡

Amendement nr. 12

Ontworpen artikel 15 van de wet van 17 januari 2003

1. Het ontworpen artikel 15, §§ 1 en 2, van de wet van 17 januari 2003 'met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector' wil het Belgisch Instituut voor Posterijen en Telecommunicatie (hierna genoemd: BIPT), in de gelegenheid stellen om, wanneer het noodzakelijk is om dat Instituut, in staat te stellen "een van zijn opdrachten inzake toepassing en controle van de bepalingen opgesomd in artikel 14, paragraaf 1, 3°, a) en g) tot i) uit te voeren", toegang te verkrijgen tot de "gegevens betreffende de abonnee of de gewoonlijke gebruiker van de dienst"[30] en tot de "andere elektronische-communicatiemetagegevens"[31] dan de gegevens betreffende de abonnee of de gewoonlijke gebruiker van de dienst.

Zoals de verantwoording van het amendement aangeeft, moet het BIPT toegang hebben tot die gegevens voor de volgende doeleinden:

> "De paragrafen 1 en 2 beogen de opdrachten inzake toepassing en controle van de naleving van de telecomwet (art. 14, § 1, 3°, a)) en van de overige sectorale wetgevingen betreffende de veiligheid van de netwerken en informatiesystemen (namelijk: art. 14, § 1, 3°, g) van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, wat betreft de sectoren van de elektronische communicatie en de kritieke infrastructuren; h) de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesstemen van algemeen belang voor de openbare veiligheid, wat de sector van de digitale infrastructuren betreft; en i) Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013 betreffende maatregelen voor het melden van inbreuken in verband met persoonsgegevens op grond van Richtlijn 2002/58/EG van het Europees Parlement en de Raad betreffende privacy en elektronische communicatie).
>
> Hetgeen deze paragrafen nastreven komt overeen met de volgende doeleinden waarin artikel 127/1, § 2, van de telecomwet voorziet:
>
> – de preventie van ernstige bedreigingen van de openbare veiligheid (art. 127[/1], § 2, 2°, van de telecomwet);
>
> – het onderzoek van veiligheidslekken inzake elektronische-communicatienetwerken of -diensten (art. 127[/1], § 2, 4°, van de telecomwet);
>
> – de controle van de telecomwet door het instituut en de controleopdrachten van de autoriteiten die bevoegd zijn voor de gegevensbescherming in het kader van hun controleopdrachten (art. 127[/1], § 2, 9° van de telecomwet)."

[30] Die gegevens zijn, overeenkomstig het ontworpen artikel 2, 5°, van de wet van 17 januari 2003 (amendement nr. 10), de "gegevens betreffende de abonnee of de gewoonlijke gebruiker van de elektronische-communicatiedienst", – bedoeld in de artikelen 126 en 127 van de wet van 13 juni 2005 'betreffende de elektronische communicatie, of ; – bewaard krachtens artikel 122 van de wet van 13 juni 2005 'betreffende de elektronische communicatie en die het mogelijk maken de abonnee of de gewone gebruiker van de dienst te identificeren".

[31] Het ontworpen artikel 2, 93°, van de wet van 13 juni 2005 definieert de elektronische-communicatiemetagegevens als volgt: "gegevens die worden verwerkt in een elektronische-communicatienetwerk met het oog op de transmissie, de distributie of de uitwisseling van elektronische-communicatie-inhoud; met inbegrip van gegevens die worden gebruikt voor de opsporing en identificatie van de bron en de bestemming van de communicatie, gegevens betreffende de locatie van de apparatuur die bij het aanbieden van elektronische-communicatiediensten worden gegenereerd, en de datum, het tijdstip, de duur en de aard van de communicatie".

‡LW-AGFWNFIFE-HBBIEUQ‡

Het BIPT zou aldus toegang kunnen krijgen tot alle opgesomde gegevens, zonder dat een onderscheid wordt gemaakt tussen de categorieën van gegevens in functie van het precieze doel dat de toegang tot die gegevens rechtvaardigt[32].

De vraag rijst of het noodzakelijk is dat het BIPT toegang heeft tot al die gegevens in het licht van de verschillende taken die aan het BIPT worden toevertrouwd.

Dat geldt *a fortiori* voor de toegang tot de elektronische-communicatiemetagegevens die, onder meer, maar niet uitsluitend, de in het ontworpen artikel 126/2, bedoelde gegevens omvatten, d.w.z. verkeers- en locatiegegevens van alle communicaties vanuit of naar een van de daarin opgelijste geografische gebieden, en derhalve gegevens die een aanzienlijke inmenging in het privéleven van de gebruikers inhouden.

De verantwoording van het amendement is in dat opzicht onvoldoende verhelderend.

Het staat aan de steller van het amendement om de elementen te kunnen vaststellen die de noodzaak en de evenredigheid kunnen rechtvaardigen van de mogelijkheid om toegang te krijgen tot al die gegevens (of een deel ervan), en dat opdracht per opdracht met inachtneming van de rechtspraak van het Hof van Justitie[33].

Het verdient aanbeveling de verantwoording van het amendement in dat opzicht aan te vullen.

Dezelfde opmerking geldt *mutatis mutandis* voor wat betreft amendement 15, dat ertoe strekt om in het ontworpen artikel 25/1 van de wet van 17 januari 2003 de officiers van gerechtelijke politie van het BIPT toegang te verlenen tot dezelfde gegevens met het oog op het onderzoek, de vaststelling of de vervolging van een inbreuk zoals bedoeld in artikel 145, § 3 of § 3*bis*, van de wet van 13 juni 2005 of in artikel 24, § 1, 2° van de wet van 17 januari 2003.

2. Het Hof van Justitie eist dat, om ervoor te zorgen dat de objectieve criteria aan de hand waarvan de omstandigheden en de voorwaarden waaronder aan de bevoegde nationale instanties toegang wordt verleend tot verkeers- en locatiegegevens, in de praktijk ten volle in acht worden genomen, het van wezenlijk belang is dat die toegang wordt onderworpen aan een voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van deze instanties[34].

Voorts heeft het Grondwettelijk Hof erop gewezen dat een dergelijke voorafgaande toetsing niet vereist is voor een verzoek om toegang tot identificatiegegevens, in tegenstelling tot een verzoek om toegang tot verkeers- en locatiegegevens[35].

[32] Zie in die zin advies 69.381/4.

[33] Zie in die zin de overwegingen 89 tot 103, van advies nr. 66/2022 van de Gegevensbeschermingsautoriteit.

[34] Overwegingen 50 en 51 van arrest C-746/18 van 2 maart 2021.

[35] Zie overweging B.16.8.6 van arrest nr. 158/2021 van 18 november 2021.

‡LW-AGFWNFIFE-HBBIEUQ‡

Er moet dus voor gezorgd worden dat de "gegevens in verband met de abonnee of de gewoonlijke gebruiker van de dienst" zoals gedefinieerd in het ontworpen artikel 2, 5°, van de wet van 17 januari 2003, waartoe het BIPT toegang kan hebben overeenkomstig het ontworpen artikel 15, § 1, enkel identificatiegegevens bevatten, zoniet zal een voorafgaande externe controle moeten worden ingevoerd om toegang te hebben tot de andere gegevens.

De verantwoording van het amendement moet dienovereenkomstig worden aangevuld.

Dezelfde opmerking geldt *mutatis mutandis* voor het ontworpen artikel 25/1, § 1, 1°, van de wet van 17 januari 2003 (amendement nr. 15).

Amendement nr. 15
Ontworpen artikel 25/1 van de wet van 17 januari 2003

In het ontworpen artikel 25/1, § 4, eerste en derde lid van de wet van 17 januari 2003 moeten de woorden "in werkelijke tijd" worden vervangen door het woord "onmiddellijk".

Het begrip "in werkelijke tijd" kan immers tot verwarring leiden, aangezien het een bijzondere betekenis kan hebben in het kader van gegevensverwerking op het gebied van elektronische communicatie[36].

Dezelfde opmerking geldt voor het ontworpen artikel 46*bis*, §§ 3 en 4, tweede lid, van het Wetboek van Strafvordering (amendement nr. 16).

Amendement n° 17
Ontworpen artikel 11 van de wet van 24 januari 1977

In het ontworpen artikel 11, § 1, elfde lid, van de wet, van 24 januari 1977 'betreffende de bescherming van de gezondheid van de verbruikers op het stuk van de voedingsmiddelen en andere produkten', dient te worden gepreciseerd dat de banktransactie voorafgaand moet zijn meegedeeld door een operator overeenkomstig de voorwaarden bepaald in de wet van 13 juni 2005.

LE GREFFIER – DE GRIFFIER LE PRÉSIDENT – DE VOORZITTER

Charles-Henri VAN HOVE Martine BAGUET

[36] Zie ter illustratie de overwegingen 183 e.v. van het arrest *La Quadrature du Net*.

‡LW-AGFWNFIFE-HBBIEUQ‡